(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号

特開平９－１２１３８８

(43)公開日　平成９年（１９９７）５月６日

(51)Int.Cl.[6]	識別記号	庁内整理番号	ＦＩ		技術表示箇所
H04Q 7/38			H04B 7/26	109 R	
G09C 1/00	610	7259-5J	G09C 1/00	610 D	
		7259-5J		610 B	
H04B 1/707			H04J 13/00	D	
H04L 9/06			H04L 9/00	611 A	

審査請求　未請求　請求項の数５５　ＯＬ　外国語出願　（全６９頁）　最終頁に続く

(21)出願番号　特願平８－２０７５３０

(22)出願日　平成８年（１９９６）７月３日

(31)優先権主張番号　４９８７１３

(32)優先日　１９９５年７月３日

(33)優先権主張国　米国（ＵＳ）

(71)出願人　３９００３５４９３
エイ・ティ・アンド・ティ・コーポレーション
ＡＴ&Ｔ　ＣＯＲＰ.
アメリカ合衆国　１００１３－２４１２
ニューヨーク　ニューヨーク　アヴェニュー　オブ　ジ　アメリカズ　３２

(72)発明者　ジェームズ　アレキサンダー　リーズ　ザ　サード
アメリカ合衆国、０７９７４　ニュージャージー、ニュープロビンス、サウスゲート　ロード　１２７

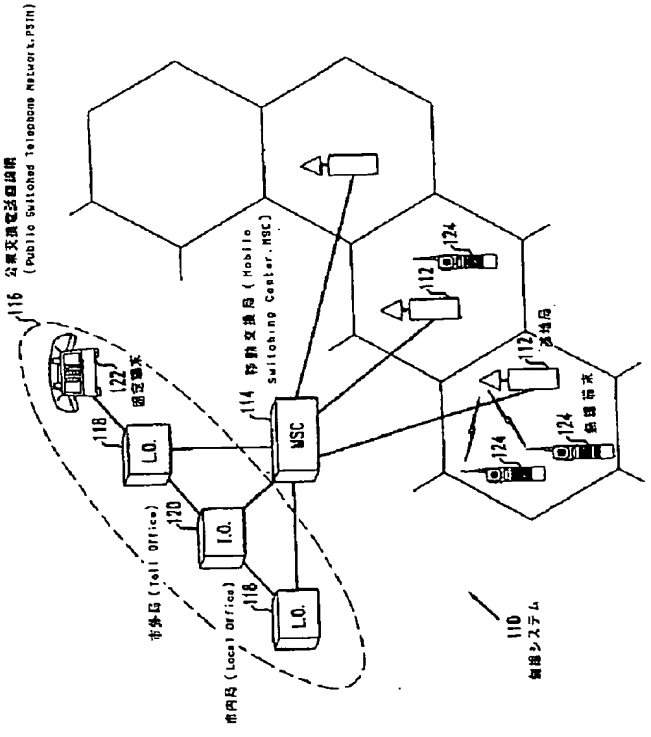
(74)代理人　弁理士　三俣　弘文

(54)【発明の名称】無線通信のための暗号システム

(57)【要約】

【課題】　プライバシー保護を必要とする無線通信用暗号システムを提供する。

【解決手段】　本発明は、プライバシー保護を必要とする無線通信システム１１０に関する。システム１１０は、基地局１１２および無線端末１２２間で暗号化された信号を伝送する。順方向通信路においては、基地局１１２は、回転する長符号マスクを生成する長符号マスク生成器２００とともに、暗号化器１３０を含んでいる。無線端末１２２は、回転する長符号マスクを創り出す長符号マスク生成器２０８とともに、復号化器１６４を、同様に含んでいる。



1

【特許請求の範囲】

【請求項１】　ＲＦアンテナと、
無線端末から信号を受信し処理するリバースチャネル回路と、
移動交換センタから無線端末への入力信号を送信する順方向チャネル回路とを有するスペクトラム拡散無線通信方式の基地局装置において、前記順方向チャネル回路は、
前記移動交換センタに応答して、前記入力信号に誤り訂正能力を与えるチャネル符号器と、
前記チャネル符号器に応答して、バースト誤りの影響を最小にするために入力信号中のビットの順序を並べ替えるビットインタリーバと、
秘密の長符号マスクと非線形関係にあるビット系列からなる鍵信号を生成する非線形スクランブラを有し、前記チャネル符号器に応答して、前記入力信号を暗号化する暗号化器と、
前記アンテナに接続され、前記チャネル符号器、前記ビットインタリーバおよび前記暗号化器に応答して、前記入力信号を変調して送信する回路とからなることを特徴とする、スペクトラム拡散無線通信方式の基地局装置。

【請求項２】　前記暗号化器は、
長符号マスクから長符号系列を生成する長符号生成器と、
前記長符号生成器に応答して、長符号マスクのビットの非線形関数である鍵信号を生成する非線形スクランブラと、
前記ビットインタリーバおよび前記非線形スクランブラに応答して、前記入力信号を暗号化する回路とからなることを特徴とする請求項１の装置。

【請求項３】　前記非線形スクランブラは、
前記長符号生成器から入力ビット列を受信する入力を有し、第１の所定数のセルを有するシフトレジスタと、
一つの出力を有し、選択されたセルの内容にアクセスするように前記シフトレジスタに接続された第１論理回路と、
前記非線形スクランブラのフィードバックループを構成するように、前記長符号生成器に接続された第１入力と、前記第１論理回路の出力に接続された第２入力と、前記シフトレジスタの入力に接続されるとともに前記非線形スクランブラの出力でもある出力を有する第２論理回路とからなることを特徴とする請求項２の装置。

【請求項４】　前記第２論理回路は排他的ＯＲゲートからなることを特徴とする請求項３の装置。

【請求項５】　前記非線形スクランブラはフィードバックループを有することを特徴とする請求項２の装置。

【請求項６】　前記非線形スクランブラは、前記非線形スクランブラの出力ビットが後続の出力ビットを生成するために使用されるようなフィードバックループを有することを特徴とする請求項２の装置。

2

【請求項７】　前記非線形スクランブラは、
前記長符号生成器から入力ビット列を受信する入力を有し、所定数のセルを有するシフトレジスタと、
前記非線形スクランブラの出力を生成するために、前記シフトレジスタの選択されたセルの内容を取り出すように接続された組合せ論理回路とからなることを特徴とする請求項２の装置。

【請求項８】　前記組合せ論理回路は、前記シフトレジスタの選択されたセルに接続された少なくとも２個の入力を有するＡＮＤゲートからなることを特徴とする請求項７の装置。

【請求項９】　前記非線形スクランブラは、
前記長符号生成器から入力ビット列を受信する入力を有し、所定数のセルを有するシフトレジスタと、
前記シフトレジスタの選択されたセルの第１のセットに接続された所定数のセレクタ入力と、前記シフトレジスタの選択されたセルの第２のセットに接続された所定数のデータ入力とを有し、前記選択されたセルの第１のセットが前記選択されたセルの第２のセットのうちから選択したセルを出力するマルチプレクサとからなることを特徴とする請求項２の装置。

【請求項１０】　前記選択されたセルの第１および第２のセットは互いに排他的であることを特徴とする請求項９の装置。

【請求項１１】　前記選択されたセルの第１および第２のセットは所定数のセルを共有することを特徴とする請求項９の装置。

【請求項１２】　前記非線形スクランブラは、
前記長符号生成器から入力ビット列を受信する入力を有し、所定数のセルを有するシフトレジスタと、
前記シフトレジスタの選択されたセルに接続された所定数の入力を有し、鍵信号を使用して、各入力ごとに暗号化出力ビットを生成するデータ暗号化規格回路と、
前記データ暗号化規格回路によって出力されたビットをそれぞれ受信するように接続された所定数のセルを有し、当該セルのうちから選択される一つのセルを前記非線形スクランブラの出力として出力するレジスタとからなることを特徴とする請求項２の装置。

【請求項１３】　前記長符号生成器に接続され、シフトレジスタを含むフィードバック回路と、
前記非線形スクランブラの出力を生成するように、前記シフトレジスタの選択されたセルを読み出すように接続された組合せ論理回路とからなることを特徴とする請求項２の装置。

【請求項１４】　スペクトル拡散無線通信方式の順方向チャネルの入力信号を暗号化する暗号化装置において、
長符号マスクから長符号系列を生成する長符号生成器と、
前記長符号生成器に応答して、長符号マスクのビットの非線形関数である鍵信号を生成する非線形スクランブラ

と、
前記入力信号を前記鍵信号で暗号化する組合せ論理回路とからなることを特徴とする、スペクトル拡散無線通信方式の順方向チャネルの入力信号を暗号化する暗号化装置。

【請求項１５】　前記非線形スクランブラは、
前記長符号生成器から入力ビット列を受信する入力を有し、第１の所定数のセルを有するシフトレジスタと、
一つの出力を有し、選択されたセルの内容にアクセスするように前記シフトレジスタに接続された第１論理回路と、
前記非線形スクランブラのフィードバックループを構成するように、前記長符号生成器に接続された第１入力と、前記第１論理回路の出力に接続された第２入力と、前記シフトレジスタの入力に接続されるとともに前記非線形スクランブラの出力でもある出力を有する第２論理回路とからなることを特徴とする請求項２の装置。

【請求項１６】　前記第２論理回路は排他的ＯＲゲートからなることを特徴とする請求項１５の装置。

【請求項１７】　前記非線形スクランブラは、前記非線形スクランブラの出力ビットが後続の出力ビットを生成するために使用されるようなフィードバックループを有することを特徴とする請求項１４の装置。

【請求項１８】　前記非線形スクランブラは、
前記長符号生成器から入力ビット列を受信する入力を有し、所定数のセルを有するシフトレジスタと、
前記非線形スクランブラの出力を生成するために、前記シフトレジスタの選択されたセルの内容を取り出すように接続された組合せ論理回路とからなることを特徴とする請求項１４の装置。

【請求項１９】　前記組合せ論理回路は、前記シフトレジスタの選択されたセルに接続された少なくとも２個の入力を有するＡＮＤゲートからなることを特徴とする請求項１８の装置。

【請求項２０】　前記非線形スクランブラは、
前記長符号生成器から入力ビット列を受信する入力を有し、所定数のセルを有するシフトレジスタと、
前記シフトレジスタの選択されたセルの第１のセットに接続された所定数のセレクタ入力と、前記シフトレジスタの選択されたセルの第２のセットに接続された所定数のデータ入力とを有し、前記選択されたセルの第１のセットが前記選択されたセルの第２のセットのうちから選択したセルを出力するマルチプレクサとからなることを特徴とする請求項１４の装置。

【請求項２１】　前記選択されたセルの第１および第２のセットは互いに排他的であることを特徴とする請求項２０の装置。

【請求項２２】　前記選択されたセルの第１および第２のセットは所定数のセルを共有することを特徴とする請求項２０の装置。

【請求項２３】　前記非線形スクランブラは、
前記長符号生成器から入力ビット列を受信する入力を有し、所定数のセルを有するシフトレジスタと、
前記シフトレジスタの選択されたセルに接続された所定数の入力を有し、鍵信号を使用して、各入力ごとに暗号化出力ビットを生成するデータ暗号化規格回路と、
前記データ暗号化規格回路によって出力されたビットをそれぞれ受信するように接続された所定数のセルを有し、当該セルのうちから選択される一つのセルを前記非線形スクランブラの出力として出力するレジスタとからなることを特徴とする請求項１４の装置。

【請求項２４】　ＲＦアンテナと、
信号を処理して基地局へ送信するリバースチャネル回路と、
基地局から送信された伝送信号を受信し処理する順方向チャネル回路とを有するスペクトラム拡散無線通信方式の無線端末装置において、前記順方向チャネル回路は、
前記アンテナに接続され、前記伝送信号を復調する受信器回路と、
秘密の長符号マスクと非線形関係にあるビット系列からなる鍵信号を生成する非線形スクランブラを有し、前記受信器回路に応答して、前記伝送信号を復号化する復号化器と、
前記受信器回路に応答して、伝送信号中のビットの順序を並べ替えるビットデインタリーバと、
前記受信器回路に応答して、前記伝送信号の誤り訂正を行うチャネル復号器と、
前記受信器回路に応答して、前記伝送信号から出力信号を生成する音声復号器と、
前記伝送信号を出力する出力デバイスとからなることを特徴とする、スペクトラム拡散無線通信方式の無線端末装置。

【請求項２５】　前記復号化器は、
長符号マスクから長符号系列を生成する長符号生成器と、
前記長符号生成器に応答して、長符号マスクのビットの非線形関数である鍵信号を生成する非線形スクランブラと、
前記非線形スクランブラおよび前記受信器回路に応答して、前記伝送信号を復号化する組合せ論理回路とからなることを特徴とする請求項２４の装置。

【請求項２６】　前記非線形スクランブラは、
前記長符号生成器から入力ビット列を受信する入力を有し、第１の所定数のセルを有するシフトレジスタと、
一つの出力を有し、選択されたセルの内容にアクセスするように前記シフトレジスタに接続された第１論理回路と、
前記非線形スクランブラのフィードバックループを構成するように、前記長符号生成器に接続された第１入力と、前記第１論理回路の出力に接続された第２入力と、

5

前記シフトレジスタの入力に接続されるとともに前記非線形スクランブラの出力でもある出力を有する第２論理回路とからなることを特徴とする請求項２５の装置。

【請求項２７】　前記第２論理回路は排他的ＯＲゲートからなることを特徴とする請求項２６の装置。

【請求項２８】　前記非線形スクランブラはフィードバックループを有することを特徴とする請求項２５の装置。

【請求項２９】　前記非線形スクランブラは、前記非線形スクランブラの出力ビットが後続の出力ビットを生成するために使用されるようなフィードバックループを有することを特徴とする請求項２５の装置。

【請求項３０】　前記非線形スクランブラは、
前記長符号生成器から入力ビット列を受信する入力を有し、所定数のセルを有するシフトレジスタと、
前記非線形スクランブラの出力を生成するために、前記シフトレジスタの選択されたセルの内容を取り出すように接続された組合せ論理回路とからなることを特徴とする請求項２５の装置。

【請求項３１】　前記組合せ論理回路は、前記シフトレジスタの選択されたセルに接続された少なくとも２個の入力を有するＡＮＤゲートからなることを特徴とする請求項３０の装置。

【請求項３２】　前記非線形スクランブラは、
前記長符号生成器から入力ビット列を受信する入力を有し、所定数のセルを有するシフトレジスタと、
前記シフトレジスタの選択されたセルの第１のセットに接続された所定数のセレクタ入力と、前記シフトレジスタの選択されたセルの第２のセットに接続された所定数のデータ入力とを有し、前記選択されたセルの第１のセットが前記選択されたセルの第２のセットのうちから選択したセルを出力するマルチプレクサとからなることを特徴とする請求項２５の装置。

【請求項３３】　前記選択されたセルの第１および第２のセットは互いに排他的であることを特徴とする請求項３２の装置。

【請求項３４】　前記選択されたセルの第１および第２のセットは所定数のセルを共有することを特徴とする請求項３２の装置。

【請求項３５】　前記非線形スクランブラは、
前記長符号生成器から入力ビット列を受信する入力を有し、所定数のセルを有するシフトレジスタと、
前記シフトレジスタの選択されたセルに接続された所定数の入力を有し、鍵信号を使用して、各入力ごとに暗号化出力ビットを生成するデータ暗号化規格回路と、
前記データ暗号化規格回路によって出力されたビットをそれぞれ受信するように接続された所定数のセルを有し、当該セルのうちから選択される一つのセルを前記非線形スクランブラの出力として出力するレジスタとからなることを特徴とする請求項２５の装置。

6

【請求項３６】　前記長符号生成器に接続され、シフトレジスタを含むフィードバック回路と、
前記非線形スクランブラの出力を生成するように、前記シフトレジスタの選択されたセルを読み出すように接続された組合せ論理回路とからなることを特徴とする請求項２５の装置。

【請求項３７】　スペクトラム拡散無線通信方式において基地局から無線端末への情報信号の傍受を防ぐ方法において、
移動交換センタから入力信号を受信するステップと、
前記入力信号をチャネル符号器で符号化することにより前記入力信号に誤り訂正能力を与えるステップと、
バースト誤りの影響を最小にするために前記入力信号のビットをビットインタリーバでインタリーブするステップと、
非線形スクランブラを有する暗号化器で、秘密の長符号マスクと非線形関係にあるビット系列からなる鍵信号を生成するステップと、
前記入力信号を前記鍵信号で暗号化するステップと、
前記入力信号を送信のために変調するステップと、
前記入力信号を送信するステップとからなることを特徴とする、スペクトラム拡散無線通信方式において基地局から無線端末への情報信号の傍受を防ぐ方法。

【請求項３８】　前記鍵信号を生成するステップは、
長符号生成器で長符号マスクから長符号系列を生成するステップと、
非線形スクランブラで前記長符号系列をスクランブルするステップとからなることを特徴とする請求項３７の方法。

【請求項３９】　前記スクランブルするステップは、フィードバックループを有する非線形スクランブラで長符号系列をスクランブルするステップからなることを特徴とする請求項３８の方法。

【請求項４０】　前記スクランブルするステップは、長符号系列を受信するように接続されたシフトレジスタと、当該シフトレジスタの選択されたセルに接続され非線形スクランブラの出力を生成する組合せ論理回路とを有する非線形スクランブラで長符号系列をスクランブルするステップからなることを特徴とする請求項３８の方法。

【請求項４１】　前記スクランブルするステップは、
所定数のセルを有するシフトレジスタを通して長符号系列のビットをシフトするステップと、
前記シフトレジスタの選択されたセルを使用して、シフトレジスタのセルのうちから前記非線形スクランブラの出力を生成するステップとからなることを特徴とする請求項３８の方法。

【請求項４２】　前記スクランブルするステップは、
所定数のセルを有するシフトレジスタを通して長符号系列のビットをシフトするステップと、

前記シフトレジスタ内のビットを、データ暗号化規格回路と、前記鍵信号とは別の鍵信号とで暗号化するステップとからなることを特徴とする請求項３８の方法。

【請求項４３】　少なくとも一つの市内局および少なくとも一つの市外局から入力信号を受信するように接続された移動交換センタと、

前記移動交換センタに接続された複数の基地局とからなるスペクトラム拡散無線通信システムにおいて、各基地局は、

ＲＦアンテナと、

無線端末から信号を受信し処理するリバースチャネル回路と、

移動交換センタから無線端末への入力信号を送信する順方向チャネル回路とを有し、当該順方向チャネル回路は、

前記移動交換センタに応答して、前記入力信号に誤り訂正能力を与えるチャネル符号器と、

前記チャネル符号器に応答して、バースト誤りの影響を最小にするために入力信号中のビットの順序を並べ替えるビットインタリーバと、

秘密の長符号マスクと非線形関係にあるビット系列からなる鍵信号を生成する非線形スクランブラを有し、前記チャネル符号器に応答して、前記入力信号を暗号化する暗号化器と、

前記チャネル符号器に応答して、前記入力信号を変調する回路とからなることを特徴とする、スペクトラム拡散無線通信システム。

【請求項４４】　前記暗号化器は、

長符号マスクから長符号系列を生成する長符号生成器と、

前記長符号生成器に応答して、長符号マスクのビットの非線形関数である鍵信号を生成する非線形スクランブラと、

前記ビットインタリーバに応答して、前記入力信号を暗号化する組合せ論理回路とからなることを特徴とする請求項４３のシステム。

【請求項４５】　前記非線形スクランブラは、

前記長符号生成器から入力ビット列を受信する入力を有し、第１の所定数のセルを有するシフトレジスタと、

一つの出力を有し、選択されたセルの内容にアクセスするように前記シフトレジスタに接続された第１論理回路と、

前記非線形スクランブラのフィードバックループを構成するように、前記長符号生成器に接続された第１入力と、前記第１論理回路の出力に接続された第２入力と、前記シフトレジスタの入力に接続されるとともに前記非線形スクランブラの出力でもある出力を有する第２論理回路とからなることを特徴とする請求項４４のシステム。

【請求項４６】　前記第２論理回路は排他的ＯＲゲートからなることを特徴とする請求項４５のシステム。

【請求項４７】　前記非線形スクランブラはフィードバックループを有することを特徴とする請求項４４のシステム。

【請求項４８】　前記非線形スクランブラは、前記非線形スクランブラの出力ビットが後続の出力ビットを生成するために使用されるようなフィードバックループを有することを特徴とする請求項４４のシステム。

【請求項４９】　前記非線形スクランブラは、

前記長符号生成器から入力ビット列を受信する入力を有し、所定数のセルを有するシフトレジスタと、

前記非線形スクランブラの出力を生成するために、前記シフトレジスタの選択されたセルの内容を取り出すように接続された組合せ論理回路とからなることを特徴とする請求項４４のシステム。

【請求項５０】　前記組合せ論理回路は、前記シフトレジスタの選択されたセルに接続された少なくとも２個の入力を有するＡＮＤゲートからなることを特徴とする請求項４９のシステム。

【請求項５１】　前記非線形スクランブラは、

前記長符号生成器から入力ビット列を受信する入力を有し、所定数のセルを有するシフトレジスタと、

前記シフトレジスタの選択されたセルの第１のセットに接続された所定数のセレクタ入力と、前記シフトレジスタの選択されたセルの第２のセットに接続された所定数のデータ入力とを有し、前記選択されたセルの第１のセットが前記選択されたセルの第２のセットのうちから選択したセルを出力するマルチプレクサとからなることを特徴とする請求項４４のシステム。

【請求項５２】　前記選択されたセルの第１および第２のセットは互いに排他的であることを特徴とする請求項５１のシステム。

【請求項５３】　前記選択されたセルの第１および第２のセットは所定数のセルを共有することを特徴とする請求項５１のシステム。

【請求項５４】　前記非線形スクランブラは、

前記長符号生成器から入力ビット列を受信する入力を有し、所定数のセルを有するシフトレジスタと、

前記シフトレジスタの選択されたセルに接続された所定数の入力を有し、鍵信号を使用して、各入力ごとに暗号化出力ビットを生成するデータ暗号化規格回路と、

前記データ暗号化規格回路によって出力されたビットをそれぞれ受信するように接続された所定数のセルを有し、当該セルのうちから選択される一つのセルを前記非線形スクランブラの出力として出力するレジスタとからなることを特徴とする請求項４４のシステム。

【請求項５５】　前記長符号生成器に接続され、シフトレジスタを含むフィードバック回路と、

前記非線形スクランブラの出力を生成するように、前記シフトレジスタの選択されたセルを読み出すように接続

された組合せ論理回路とからなることを特徴とする請求項４４のシステム。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、通信の分野に関し、特に、無線通信用暗号システムに関する。

【０００２】

【従来の技術】毎日、何百万人ものユーザが、無線システムを用いて、通信を行っている。このような通信は、音声およびデータ伝送を含むものである。これらのシステムのユーザのすべてではないにしても、ほとんどは、通信の内容が公然に得られるものとなることを望んではいない。むしろ、一般には、ユーザは通信の内容を、秘密に保っておくことを望んでいるといえる。残念なことに、暗号によって適切な保護措置がなされないことには、侵入者は、ある種の無線システムにおける通信を容易に盗聴可能である。例えば、ほとんどのアナログ無線システムは、傍受から通信を保護することを行っていない。盗聴者は、単に適切な周波数に受信器（ラジオ）を合わせる（チューニングする）ことで、伝送内容にアクセス可能である。

【０００３】現在のデジタル無線通信システムのなかには、ユーザのプライバシーを保護する保護措置をとっているものもある。例えば、米国電気通信産業協会(Telecommunication Industry Association)では、スペクトル拡散無線通信システムのための標準を起案している。この標準案の現時点での版（ヴァージョン）は、PN-3421と記された（IS-95aとして公表される）Mobile Station-Base Station Compatibility Standard for Dual-Mode Spread Spectrum Cellular Systemとして、1994年12月に発行された（以降、標準案と称する）。標準案で記述されたスペクトル拡散システムは、通常の言葉では、符号分割多重アクセス(Code Division Multiple Access)あるいはＣＤＭＡと称されている。標準案では、プライバシーを増すため、伝送に先だって、音声あるいはデータ信号を暗号化する計画を含んでいる。このように、音声あるいはデータの伝送の真の受け取り手のみが、伝送内容を得るべきである。

【０００４】

【発明が解決しようとする課題】標準案により特定されている暗号システムにおいて、これまで認識されていなかった問題は、標準案に従って暗号化された伝送を、盗聴者が、容易にかつすばやく、暗号解析（暗号解読）を行い、それにより伝送内容にアクセスすることを許容しているということにある。標準案で記述された順方向トラヒック通信路（チャネル）は、伝送に先立ち、キー信号（鍵信号）をもって、入力音声あるいはデータ信号を暗号化することを必要としている。また、標準案は、入力信号が、排他的ＯＲ関数（すなわち、ｍｏｄ２、つまり、２を法として加える）により、長符号配列と結合され、暗号化された出力信号を生成することを特定している。

【０００５】標準案は、公然に知られた配列と、長符号マスクとして知られる、専用の４２ビットのパターンから、長符号配列を生成することを要する。公然に利用可能な配列は、線形帰送りレジスタ（線形シフトレジスタ）として概念化されることの可能なものに配置されている。線形帰送りレジスタの出力は、長符号マスクのビットと結合される。結合の線形的な性質のため、長符号配列は、専用の長符号マスクのビットに線形に依存している。このことより、盗聴者が、長符号配列の４２ビットへアクセスすることで、無線通信を復号化することを可能にしている。盗聴者は、長符号マスクの未知の４２ビットに依存している４２の線形方程式を創り出すため、長符号配列からのビットを利用することが可能であろう。しかしながら、標準案では、長符号配列のビットの直接の伝送を要求していない。さらに、排他的ＯＲ関数は、長符号配列のビットと未知の入力信号とを結合させるもので、このようにすることで、長符号配列を転化させる。このことは、盗聴者が、うまく暗号化された伝送を暗号解析（暗号解読）する機会を、最小限にするはずである。標準案については、（ただし）この点は当てはまらない。それは、入力信号が、誤り訂正のため、３８４ビットのフレームを形成するように処理されるという方法をとっていることによる。

【０００６】盗聴者は、入力信号の各フレームにおける最後の１６ビット内の関係を認識することで、暗号化された伝送を暗号解析（暗号解読）することが可能である。特定するに、盗聴者は、２を法とする（モジュロ２の）数の合計が０を生成するように、各フレームにおける最後の１６ビットから選択された、入力信号のビットを結合することが可能である。対応する入力ビットの合計が０であるような、出力信号の（ｍｏｄ２による）ビットを加えることで、盗聴者は、長符号配列のビットの結合を表しているデータを得ることが可能である。実質的には、盗聴者は、出力信号への入力信号の影響をキャンセルすることが可能である。長符号配列の各ビットは、４２ビットの長符号マスクに線形に依存している。このようなことから、長符号マスクのビットに線形に依存している方程式を創り出すため、盗聴者は、出力信号の既知のビットを結合することが可能である。データについての連続するフレームが、通信が開始した後、１秒以下以内に、通信の復号化（暗号解読）を許容するような４２の方程式を生じさせる。

【０００７】

【課題を解決するための手段】本発明の実施例は、実質的には、暗号化された伝送について暗号解析（暗号解読）する、盗聴者の能力を排除あるいは減少させるものである。特定するに、本発明の典型的な実施例は、長符号生成器の出力に接続された非線形スクランブラを含ん

でいる。これにより、デシメートされた（大幅に減らされた）長符号配列から線形性を取り除き、長符号マスクを決定して、従って、暗号化された出力信号について暗号解析（暗号解読）することをより困難とするものである。

【発明の実施の形態】

【０００８】米国電気通信産業協会（The Telecommunication Industry Association, ＴＩＡ）は、無線通信システムのための標準を設定している。ＴＩＡは、スペクトル拡散無線通信システム用の基準を起案している。標準案で記述されたシステムは、符号分割多重化アクセス（Code Division Multiple Access, ＣＤＭＡ）と呼ばれている。標準案の一部では、無線通信におけるプライバシーの必要性を論じている。標準案の現時点での版（ヴァージョン）は、PN-3421と記された（IS-95aとして公表される）Mobile Station-Base Station Compatibility Standard forDual-Mode Spread Spectrum Cellular Systemとして、1994年12月に発行された。（以降、標準案と称する。）以下で概説されたような標準案の詳細な分析を元にすると、標準案に従って組み立てられた通信システムは、暗号システムの設計において、以前は未知であった脆弱性のため、その暗号処理手順にもかかわらず、盗聴者による攻撃を受けやすい。本発明の実施例は、暗号化された通信へのセキュリティを増した、順方向通信路回路およびその方法を備えることで、標準案の暗号処理手順におけるこのような脆弱性に打ち勝つことを可能とするものである。

【０００９】標準案で特定された順方向通信路回路を詳細に検討することは、本暗号化システムの脆弱性についての理解を提供するものといえる。図１は、標準案に従った、基地局における１０で一般的に示された、順方向通信路回路のブロック線図である。順方向通信路回路１０は、典型的には、通信路符号器（チャネル符号器１２、ブロックインタリーバ１４、線形暗号器１６を含んでいる。

【００１０】通信路符号器１２は、デジタル入力信号Ｉを処理する。例えば、入力信号Ｉは、無線ネットワークにおける、符号化されたデジタル音声、データ、あるいは伝送のための、その他の適切な信号を含みうる。通信路符号器１２、およびブロックインタリーバ１４は、信号Ｉの連続するビットが、伝送の間に失われたり、飛ばされたりしているとき、順方向通信路回路１０の出力への影響を最小化する。通信路符号器１２は、典型的には、フレーム特性（フレームクオリティ）指示器１８、後部符号器２０、畳込み符号器２２、記号反復回路２４の直列な結合を含んでいる。ブロックインタリーバ１４とともに、通信路符号器１２は、処理された信号Ｅを出力する。

【００１１】線形暗号器１６は、キー信号Ｇを生成し、処理された信号Ｅを暗号化する。線形暗号器１６は、典型的には、デシメータ２８と長符号生成器２６の直列な結合を含んでいる。長符号生成器２６は、長符号マスクと呼ばれる、専用の入力信号Ｍからビット配列を生成する。長符号生成器２６による出力である、信号Ｆは、長符号配列と呼ばれている。デシメータ回路２８は、長符号配列のビットの６４のうち一つを信号Ｇとして出力する。デシメータ２８の出力は、排他的ＯＲ関数のような、モジュロ２の（２を法とする）加算器の入力に結合されている。通信路符号器１２は、また、モジュロ２の（２を法とする）加算器３０の入力に結びつけられている。モジュロ２の（２を法とする）加算器３０は、信号Ｅの暗号化されたものを多重化器３２へと出力する。出力制御ビット信号ＰＣＢは、また、多重化器３２に供給されている。多重化器３２は、信号Ｏを図１の順方向通信路回路１０の出力として出力する。デシメータ３３は、デシメータ２８と多重化器３２の制御入力の間に結びつけられている。

【００１２】動作中は、順方向通信路回路１０は、入力信号Ｉを受け取り、処理して、伝送用の暗号化された出力信号Ｏを供給している。入力信号Ｉは、ビットのフレームとして受け取られる。各フレームにおけるビット数は、入力信号に含まれた情報を元に変化しうる。例えば、最大データレートの場合における各フレームは、１７２ビットであるが、一方では、最も低いデータレートの場合においては、各フレームは、わずか１６ビットしか含まない。記号反復回路２４は、各データレートの場合の信号Ｅにおける全体のビット数が同じとなるように、畳込み符号器２２の出力を複製する。以下の分析における助けとするため、信号Ｅ、Ｇ、Ｏは、長さ３８４ビットのバイナリベクトルとみなされる。また、各ベクトルは、２つの下付き添字を有している。第一の添字ｆは、ベクトルを生成する際のデータのフレームを示すものであり、第二の添字ｊは、ベクトルの要素あるいはビットを示すものである。

【００１３】通信路符号器１２は、入力信号Ｉを操作し、伝送の間に生じるバーストエラーの影響を低減させる。フレーム特性（フレームクオリティ）指示器１８は、入力信号Ｉの各フレーム末端位に所定数のビットを添加することで、最初に信号Ａを創り出す。後部符号器２０は、０に等しい８ビットの後端部のセットを添加することで、信号Ｂを創り出す。畳込み符号器２２は、信号Ｂの２倍のビットをもつ信号Ｃを創り出す。典型的な畳込み符号器は、図２における２２ａで一般的に示されている。畳込み符号器２２ａは、後部符号器２０から信号Ｂを受け取る線形術送りレジスタ（シフトレジスタ）３４を含んでいる。信号Ｂの現時点でのビット同様、ビット位置３４ａ、３４ｂ、３４ｃ、３４ｅ、３４ｇおよび３４ｈは、排他的ＯＲ関数のような、モジュロ２の（２を法とする）加算器３６に結びつけられており、畳込み符号器２２ａの第一の出力を提供する。さらに、信

13

号Ｂの現時点でのビット同様、ビット位置３４ｂ、３４ｃ、３４ｄ、３４ｈは、排他的ＯＲ関数のような、モジュロ２の（２を法とする）加算器３８に結びつけられており、畳込み符号器２２ａの第二の出力を提供する。インタリーバ３９は、畳込み符号器２２ａの２つの出力をインタリーブして、出力信号Ｃを提供する。このようなことから、畳込み符号器２２ａの出力ビットである、信号Ｃは、信号Ｂのビットの線形結合、例えば、モジュロ

14

２での（２を法とする）合計である。記号反復回路２４およびブロックインタリーバ１４は、さらに信号Ｃを操作して、信号Ｅを生成する。信号Ｅのビットは、２４ビットの１６グループで配列されている。最大データレートの場合において、信号Ｅのビットは、以下の表１で示されている。

【表１】

表１－最大レート（最大データレート）の場合の、インタリーバ１４のインタリーブ（交互配置）パターン

1	9	5	13	3	11	7	15	2	10	6	14	4	12	8	16
65	73	69	77	67	75	71	79	66	74	70	78	68	76	72	80
129	137	133	141	131	139	135	143	130	138	134	142	132	140	136	144
193	201	197	205	195	203	199	207	194	202	198	206	196	204	200	208
257	265	261	269	259	267	263	271	258	266	262	270	260	268	264	272
321	329	325	333	323	331	327	335	322	330	326	334	324	332	328	336
33	41	37	45	35	43	39	47	34	42	38	46	36	44	40	48
97	105	101	109	99	107	103	111	98	106	102	110	100	108	104	112
161	169	165	173	163	171	167	175	162	170	166	174	164	172	168	176
225	233	229	237	227	235	231	239	226	234	230	238	228	236	232	240
289	297	293	301	291	299	295	303	290	298	294	302	292	300	296	304
353	361	357	365	355	363	359	367	354	362	358	366	356	364	360	368
17	25	21	29	19	27	23	31	18	26	22	30	20	28	24	32
81	89	85	93	83	91	87	95	82	90	86	94	84	92	88	96
145	153	149	157	147	155	151	159	146	154	150	158	148	156	152	160
209	217	213	221	211	219	215	223	210	218	214	222	212	220	216	224
273	281	277	285	275	283	279	287	274	282	278	286	276	284	280	288
337	345	341	349	339	347	343	351	338	346	342	350	340	348	344	352
49	57	53	61	51	59	55	63	50	58	54	62	52	60	56	64
113	121	117	125	115	123	119	127	114	122	118	126	116	124	120	128
177	185	181	189	179	187	183	191	178	186	182	190	180	188	184	192
241	249	245	253	243	251	247	255	242	250	246	254	244	252	248	256
305	313	309	317	307	315	311	319	306	314	310	318	308	316	312	320
369	377	373	381	371	379	375	383	370	378	374	382	372	380	376	384

【００１４】表１における数は、畳込み符号器２２からの信号Ｃでのビット位置を呼称しているということが認められる。さらに、表１における各カラム（列）は、２４ビットの１６グループのうちの一つを表している。通信路符号器１２の動作は、公開されており、従って、潜在的な盗聴者は、表１において含まれた情報にはアクセスが可能である。

【００１５】線形暗号器１６は、信号Ｅと合計される（２を法として）信号Ｇを創り出す。長符号生成器２６は、専用の長符号マスクＭから、推定上、専用とされる長符号配列を創り出している。２６ａで一般的に示された、典型的な長符号生成器は、図３に示されている。長符号生成器２６ａは、４２ビットを有する、公然に知られた量を含む線形フィードバック桁送りレジスタ（線形フィードバックシフトレジスタ）４０を含んでいる。桁送りレジスタの各ビットは、対応するＡＮＤゲート４２

15

において、専用長符号マスクMの対応するビットと結合される。各ＡＮＤゲートの出力は、加算器４４と結び付けられている。加算器４４は、モジュロ２の（２を法とする）、あるいは排他的ＯＲの、加算器を含んでいる。

$$F_{f,j} = \sum_i m_i x_{i,f,j}$$

ここで、x～｛i，f，j｝とは、f番目のフレームの処理の間にj回ステップをえた後の、線形フィードバック桁送りレジスタ４０のi番目のセルの内容であり、m～｛i｝とは、長符号マスクのi番目のビットであり、F～｛f，j｝とは、f番目のフレームの開始からの、長符号配列のj番目のビットである。デシメータ２８

$$G_{f,j} = \sum_i m_i x_{i,f,(64j)}$$

【００１６】ブロックインタリーバ１４からの信号Eは、モジュロ２の（２を法とする）加算器３０において、線形暗号器１６の信号Gと、モジュロ２として（２を法として）合計される。信号Eは、モジュロ２とする（２を法とする）算術で、信号Gに加算される。モジュロ２の（２を法とする）加算器３０による、各ビット出力について、多重化器３２は、モジュロ２の（２を法とする）加算器３０の出力、あるいはＰＣＢ信号を、順方向通信路回路１０の出力信号Oとして伝送する。ＰＣＢ信号は、信号Eでの２４ビットの各グループにおける最初の１７ビットの対を上書きする出力制御信号である。従って、信号Oでの２４ビットの各グループについての最後の７ビットのみが、ＰＣＢ信号の影響からフリーである。（影響を受けない。）

【００１７】伝送を暗号化するため用いられる長符号配列Fは、長符号マスクM（式１での）に線形に依存している。さらに、信号Dのビットが、既知の線形代数方程式により、信号Iのビットと関連付けられているように、通信路符号器１２は、入力信号Iのビットを操作している。従って、潜在的な盗聴者が、入力信号Iの影響を取り除くように、出力信号Oを操作することが可能であるとすれば、その盗聴者は、長符号マスクMの未知のビットに線形に依存するデータを有することになるであろう。このようなデータをもって、盗聴者は、長符号マスクMを決定するため、線形方程式を解く標準的な技術を利用することが可能となる。

【００１８】通信路符号器１２による信号Eの出力ビット

$$\langle \alpha, E_f \rangle = 0$$

式（４）は、ベクトルαとEの、モジュロ２での（２を法としての）ドット積（内積）を指していることが示されている。ベクトルαでは、Eとのドット積（内積）が、０に等しい、Eのビット合計を創り出すように、ビットが選択される。式（３）における各ベクトルとαのドット積（内積）をとると、次式のようになる。

16

加算器４４は、ＡＮＤゲート４２の出力を共に加算し、長符号配列Fのビットを生成する。FとMの間の関係は、次式のように表現されることが可能である。

【数１】

$$(1)$$

は、信号Fの全部で６４ビットのうち一つを、信号Eを暗号化するため利用される信号Gとして出力する。従って、信号Gの各ビットは、また、次式のように表現されることが可能である。

【数２】

$$(2)$$

トは、長符号マスクMのビットのみに依存する線形方程式を創り出すように結合されることが可能である。このような関係をみるため、順方向通信路回路１０の数学的記述を考えてみよう。まずは、（簿記を付けるように）詳細な表記を行う。ＰＣＢ信号の影響のため、盗聴者が頼りにできる唯一のビットは、出力信号Oでの２４ビットの各グループの内、最後の７ビットである。従って、f番目のフレームで、ビットの各グループの最後の７ビットに属するすべてのビット位置jについて、順方向通信路回路１０の出力は、以下の等式で記述可能である。

【数３】

$$E_{f,j} \oplus G_{f,j} = O_{f,j}$$

各フレームにおいて、式（３）は、順方向通信路回路１０への信号Ｉ入力の１１２ビットの値を支配している。上の式（２）は、Gが、長符号マスクの未知のビットm～｛i｝に依存していることを示している。ベクトルEは、盗聴者にとっては知られていない。従って、m～｛i｝にのみ依存する方程式を創り出すため、ベクトルEの影響が取り除かれなくてはならない。２４ビットの各グループにおける最初の１７ビットのなかで、jのすべての値について、α～｛j｝が0となり、次式が成り立つように、ベクトルαが見いだされることが可能であるとすれば、出力ベクトルOへのEの影響は取り除かれることが可能である。

【数４】

$$(4)$$

【数５】

$$\langle \alpha, E_f \rangle \oplus \langle \alpha, G_f \rangle = \langle \alpha, O_f \rangle$$

式（４）を、式（５）に代入すると、次式のようになる。

【数６】

17

$$\langle \alpha, G_f \rangle = \langle \alpha, O_f \rangle \tag{6}$$

18

式（２）において、上で議論されたように、信号Ｇは、信号Ｆのデシメートされたものであり、従って、各ビットは、長符号マスクｍ～｛ｉ｝のビットに線形に依存している。このようなことから、式（６）は、以下の次式のように展開することが可能である。

【数７】

$$\sum_j \alpha_j \sum_i m_i x_{i,f,(64j)} = \sum_j \alpha_j O_{f,j} \tag{8}$$

これは、線形方程式であり、ここで、長符号マスクのビットｍ～｛ｉ｝は、唯一の未知のものである。従って、４２の方程式を生成するため、十分なデータが集められているとすれば、盗聴者は、長符号マスクのビットを決定するために既知の技術を利用することが可能である。盗聴者は、最初に式（３）を満たすベクトルαを識別しなくてはならない。通信路符号器１２は、このことを可能にするものである。

【００１９】式（３）を満たすベクトルαを見つけるため、畳込み符号器２２を通じて、信号Ｂでのデータの最後の１６ビットをトレースする。ここで、最後の８ビットについては、後部符号器２０により設定されたものとして、０となっているものとしよう。さらに、先の方の８ビットは、ａ、ｂ、ｃ、ｄ、ｅ、ｆ、ｇ、ｈであり、ここで、ａとは、８つの０というビットが（後に）続いているビットであるものとしよう。すると、信号Ｃの最後の１６ビットは、以下のようになる。

【数９】

$$c_{369} = a \oplus b \oplus c \oplus e \oplus g \oplus h \tag{9}$$

$$c_{370} = b \oplus c \oplus d \oplus h \tag{10}$$

$$c_{371} = a \oplus b \oplus d \oplus f \oplus g \tag{11}$$

$$c_{372} = a \oplus b \oplus c \oplus g \tag{12}$$

$$c_{373} = a \oplus c \oplus e \oplus f \tag{13}$$

$$c_{374} = a \oplus b \oplus f \tag{14}$$

$$c_{375} = b \oplus d \oplus e \tag{15}$$

$$c_{376} = a \oplus e \tag{16}$$

$$c_{377} = a \oplus c \oplus d \tag{17}$$

$$c_{378} = d \tag{18}$$

$$c_{379} = b \oplus c \tag{19}$$

$$c_{380} = c \tag{20}$$

$$c_{381} = a \oplus b \tag{21}$$

$$c_{382} = b \tag{22}$$

$$c_{383} = a \tag{23}$$

$$c_{384} = a \tag{24}$$

【００２０】モジュロ２の（２を法とする）数の合計が０を生じる、信号Ｃのビットの結合は、式（３）を満たしている。例えば、ビットｃ～｛３８３｝およびｃ～｛３８４｝の合計は、それらのビットが等しいことから、０である。記号反復およびインタリーブの後には、信号Ｃのビット３８３および３８４は、それぞれ、信号Ｅのビット１９２と３８４とになることが認められる。従って、結果としてこれらの２つのビットの合計となるベクトルαは、次式のように、長符号マスクＭのビットｍ～｛ｉ｝における線形方程式を生じるであろう。

【数１０】

$$G_{f,192} \oplus G_{f,384} = O_{f,192} \oplus O_{f,384} \tag{25}$$

19　　20

式（２５）は、次のように書き換え可能である。　　【数１１】

$$\sum_i m_i\left(x_{i,f,(64\cdot192)} \oplus x_{i,f,(64\cdot384)}\right) = O_{f,192} \oplus O_{f,384} \qquad (26)$$

【００２１】式（２６）において、唯一の未知のものは、長符号マスクのビットm～｛i｝である。結果としてベクトルαとなる、その他の結合は、以下のようなものである。　　【数１２】

$$c_{369} \oplus c_{370} \oplus c_{371} \oplus c_{373} \oplus c_{379} \oplus c_{383} = 0 \qquad (27)$$

$$c_{377} \oplus c_{378} \oplus c_{379} \oplus c_{381} = 0 \qquad (28)$$

$$c_{373} \oplus c_{374} \oplus c_{375} \oplus c_{377} \oplus c_{383} = 0 \qquad (29)$$

$$c_{381} \oplus c_{382} \oplus c_{383} = 0 \qquad (30)$$

$$c_{371} \oplus c_{372} \oplus c_{373} \oplus c_{375} \oplus c_{381} = 0 \qquad (31)$$

$$c_{379} \oplus c_{380} \oplus c_{381} \oplus c_{383} = 0 \qquad (32)$$

$$c_{375} \oplus c_{376} \oplus c_{377} \oplus c_{379} = 0 \qquad (33)$$

従って、最大（データ）レートの場合において、盗聴者は、一つのデータフレームから、出力信号Ｏへの入力信号Ｉの影響をキャンセルする、少なくとも８つのビットの結合を創り出すことが可能である。丁度６つのデータフレームをもって、盗聴者は、長符号マスクＭの４２ビットの値を決定するために必要な４２の以上の方程式を創り出すことが可能である。このようなデータは、１秒以下以内に集められることが可能である。より低い（データ）レートの場合においては、盗聴者の手間はいくらか単純化される。以下の表２は、信号Ｅのビットを、畳込み符号器による信号Ｃの出力における（番号と同じ）ように、各ビットに対するビット位置の番号とともに示している。

【表２】

21　　22

表２－低いレート（低いデータレート）の場合の、インタリーバ１４のインタリーブ（交互配置）パターン

1	2	1	2	1	2	1	2	1	2	1	2	1	2	1	2
9	10	9	10	9	10	9	10	9	10	9	10	9	10	9	10
17	18	17	18	17	18	17	18	17	18	17	18	17	18	17	18
25	26	25	26	25	26	25	26	25	26	25	26	25	26	25	26
33	34	33	34	33	34	33	34	33	34	33	34	33	34	33	34
41	42	41	42	41	42	41	42	41	42	41	42	41	42	41	42
5	6	5	6	5	6	5	6	5	6	5	6	5	6	5	6
13	14	13	14	13	14	13	14	13	14	13	14	13	14	13	14
21	22	21	22	21	22	21	22	21	22	21	22	21	22	21	22
29	30	29	30	29	30	29	30	29	30	29	30	29	30	29	30
37	38	37	38	37	38	37	38	37	38	37	38	37	38	37	38
45	46	45	46	45	46	45	46	45	46	45	46	45	46	45	46
3	4	3	4	3	4	3	4	3	4	3	4	3	4	3	4
11	12	11	12	11	12	11	12	11	12	11	12	11	12	11	12
19	20	19	20	19	20	19	20	19	20	19	20	19	20	19	20
27	28	27	28	27	28	27	28	27	28	27	28	27	28	27	28
35	36	35	36	35	36	35	36	35	36	35	36	35	36	35	36
43	44	43	44	43	44	43	44	43	44	43	44	43	44	43	44
7	8	7	8	7	8	7	8	7	8	7	8	7	8	7	8
15	16	15	16	15	16	15	16	15	16	15	16	15	16	15	16
23	24	23	24	23	24	23	24	23	24	23	24	23	24	23	24
31	32	31	32	31	32	31	32	31	32	31	32	31	32	31	32
39	40	39	40	39	40	39	40	39	40	39	40	39	40	39	40
47	48	47	48	47	48	47	48	47	48	47	48	47	48	47	48

各ビットは、８回繰り返されていることが認められる。従って、低い（データ）レートの場合は、盗聴者は、単一のデータフレームをもって、長符号マスクMのビットを決定することが可能である。このように、低い（データ）レートの場合においては、長符号マスクMのビットを決定する方程式を創り出すことは、より容易である。

【００２２】図４は、１１０において一般的に示され、スペクトル拡散技術を実施しており、本発明の教示するところに従って構成された、無線システムのブロック線図である。無線システム１１０は、移動交換局（Mobile Switching Center, ＭＳＣ）１１４に結びつけられ、それと通信している、複数の基地局１１２を含んでいる。ＭＳＣ１１４は、一つ以上のローカル局（市内局）１１８と一つ以上の市外局１２０を含む公衆交換電話回線網（public switched telephone network, ＰＳＴＮ）に結びつけられ、それと通信している。ＰＳＴＮ１１６は、さらに、ローカル局（市内局）１１８および市外局１２０に結びつけられ、それと通信している固定端末１２２を含んでいる。固定端末は、例えば、銅線、光ファイバーケーブル、およびそれに類するものを含む、任意の適切な通信ケーブルにより、ＰＳＴＮに結びつけられうる。また、無線システム１１０は、一つ以上の無線端末１２４を含んでいる。各無線端末１２４および各基地局１１２の順方向通信路は、従来のシステムおよび方法と比較して、伝送におけるプライバシーの増加を提供するため、以下で記述されたような暗号化器を含んでいる。

【００２３】動作中は、無線システム１１０は、基地局１１２と無線端末１２４との間で暗号化された信号を伝送する。例えば、無線端末１２４への通信は、固定端末１２２において開始されうる。ローカル局（市内局）１

１８とＭＳＣ１１４は、固定端末１２２を適切な基地局１１２へと接続する。基地局１１２は、固定端末１２２からの信号を暗号化し、その暗号化された信号を伝送する。適切な無線端末１２４は、暗号化された信号を受け取る。無線端末１２４は、信号を復号化して、通信を完了する。

【００２４】図５は、１１２において一般的に示され、本発明の教示するところに従って構成された、基地局の一つの実施例のブロック線図である。基地局１１２は、無線端末１２４へと信号を伝送する順方向通信路１２６を含んでいる。また、基地局１１２は、無線端末１２４からの信号を受け取る逆監視通信路（リバースチャネル）１２８を含んでいる。順方向通信路１２６は、専用長符号マスクの非線形関数であるキー信号を創り出す暗号化器１３０を含んでいる。従って、順方向通信路１２６は、伝送におけるプライバシーの増加を提供している。

【００２５】順方向通信路１２６は、ＭＳＣ１１４に結びつけられている通信路符号器１３２を含んでいる。順方向通信路１２６は、さらに、ビットインタリーバ１３４、暗号化器１３０、ウォルシュ関数変調器１３６、直角位相（直交位相）拡散器１３８、直角位相（直交位相）搬送波変調器１４０、ＲＦ送信器１４２の直列の結合を含んでいる。ＲＦ送信器１４２はアンテナ１４４に結びつけられている。逆監視通信路（リバースチャネル）１２８は、ＲＦ受信器１４６、直角位相（直交位相）搬送波復調器１４８、直角位相（直交位相）逆拡散器１５０、逆拡散器１５２、ウォルシュ記号復調器１５４、ビットデインタリーバ１５６、通信路復号器（チャネル復号器）１５８の直列の結合を含んでいる。

【００２６】動作中は、順方向通信路１２６は、アンテナ１４４での伝送のために、ＭＳＣ１１４からの信号を処理し、暗号化する。ＭＳＣ１１４は、デジタル信号を通信路符号器１３２に供給する。通信路符号器１３２は、伝送後の誤り訂正のために信号を符号化している。ビットインタリーバ１３４は、エラーバーストの影響を最小限化するように、信号のビット配列を再配置する。暗号化器１３０は、ビットインタリーバ１３４からの信号を暗号化するため、非線形のキー信号を利用している。ウォルシュ関数変調器１３６は、選択されたウォルシュ関数を信号に掛けることで、信号を変調する。直角位相拡散器１３８は、固定端末１２２と無線端末１２４間の伝送に固有の、選択されたＰＮ(pseudo-noise)符号をもって信号を拡散する。直角位相搬送波変調器１４０は、アンテナ１４４での、ＲＦ送信器１４２による伝送のため信号を変調する。

【００２７】逆監視通信路（リバースチャネル）１２８は、アンテナ１４４および受信器１４６において、無線端末１２４から信号を受信する。直角位相搬送波変調器１４８は、処理のため、搬送波から信号を復調する。直

角位相逆拡散器１５０は、適切なＰＮ信号を用いて、無線端末１２４からの信号を逆拡散する。逆拡散器１５２は、専用キー信号を用いて、さらに無線端末１２４からの信号を逆拡散する。ウォルシュ記号復調器１５４は、適切なウォルシュ関数をもって、信号を復調する。ビットデインタリーバ１５６は、信号におけるビットを再配置し、無線端末１２４により実行されたインタリーブ（交互配置）操作を元に戻す。通信路復号器１５８は、誤り訂正技術を用いて、無線端末１２４からの信号における誤りを訂正する。

【００２８】図６は、１２４において一般的に示され、本発明の教示するところに従って構成された、無線端末のブロック線図である。無線端末１２４は、基地局１１２へ信号を伝送する逆監視通信路（リバースチャネル）１６０を含んでいる。また、無線端末１２４は、基地局１１２から信号を受信する順方向通信路１６２を含んでいる。順方向通信路１６２は、専用長符号マスクの非線形関数であるキー信号を創り出す復号化器１６４を含んでいる。従って、順方向通信路１６２は、伝送におけるプライバシーの増加を提供している。

【００２９】無線端末１６８は、入出力（Ｉ／Ｏ）装置１６６を含んでいる。入出力（Ｉ／Ｏ）装置１６６は、スピーカーおよびマイクロフォンを含みうる。選択的には、入出力（Ｉ／Ｏ）装置１６６は、適切なデータポートを含みうる。逆監視通信路（リバースチャネル）１６０は、入出力（Ｉ／Ｏ）装置１６６に結びつけられた音声符号器１６８を含んでいる。音声符号器１６８は、通信路符号器１７０、ビットインタリーバ１７２、ウォルシュ関数変調器１７４、拡散器１７６、直角位相拡散器１７８、直角位相搬送波変調器１８０、ＲＦ送信器１８２の直列の結合に結びつけられている。ＲＦ送信器１８２は、アンテナ１８４に結びつけられている。逆監視通信路（リバースチャネル）１６２は、ＲＦ受信器１８６、直角位相搬送波復調器１８８、直角位相逆拡散器１９０、ウォルシュ関数変調器１９２、復号化器１６４、ビットデインタリーバ１９４、通信路復号器１９６、音声復号器１９８の直列の結合に結びつけられている。音声復号器１９８は、入出力（Ｉ／Ｏ）装置１６６に結びつけられている。

【００３０】動作中は、逆監視通信路（リバースチャネル）１６０は、アンテナ１８４での伝送のため、ユーザからの信号を処理する。音声符号器１６８は、入出力（Ｉ／Ｏ）装置１６６からのデジタル信号を符号化する。通信路符号器１７０は、伝送の後の誤り訂正のため信号を符号化する。ビットインタリーバ１７２は、誤りバーストの影響を最小限化するように、信号におけるビット配列を再配置する。ウォルシュ関数変調器１７４は、選択されたウォルシュ関数を信号に掛けることで、信号を変調する。拡散器１７６は、キー信号を用いて、ウォルシュ関数変調器１７４からの信号を拡散する。直

25

角位相拡散器１７８は、固定端末１２２と無線端末１２４の間の伝送に固有の、選択されたＰＮ(pseudo-noise)符号をもって信号を拡散する。直角搬送波変調器１８０は、アンテナ１８４での、ＲＦ送信器１８２による伝送のため信号を変調する。

【００３１】順方向通信路１６２は、アンテナ１８４および受信器１８６において、基地局１１２から信号を受信する。直角位相搬送波変調器１８８は、処理のため、搬送波から信号を復調する。直角位相逆拡散器１９０は、適切なＰＮ信号を用いて、基地局１１２からの信号を逆拡散する。ウォルシュ関数復調器１９２は、適切なウォルシュ関数をもって、信号を復調する。復号化器１６４は、専用キー信号を用いて、基地局１１２からの信号についてスクランブルを解く。ビットデインタリーバ１９４は、信号におけるビットを再配置し、基地局１１２により実行されたインタリーブ（交互配置）操作を元に戻す。通信路復号器１９６は、誤り訂正技術を用いて、基地局１１２からの信号における誤りを訂正する。音声復号器１９８は、入出力（Ｉ／Ｏ）装置１６６への信号を復号し、伝送を完了させる。

【００３２】図7は、１３０において一般的に示された、図５の順方向通信路１２６で用いられる、暗号化器の実施例である。暗号化器１３０は、長符号マスク生成器２００、長符号生成器２０２、デシメータ２０４の直列の結合をもって、キー信号を生成する。デシメータ２０４の出力は、モジュロ２の（２を法とする）加算器２０６の第一の入力に結びつけられている。加算器２０６の第二の入力はビットインタリーバ１３４に結びつけられている。

【００３３】動作中は、長符号マスク生成器２００は、長符号マスクと呼ばれるビット配列を生成する。長符号生成器２００は、長符号配列のビットが長符号マスクのビットに線形に依存するような、図３の長符号生成器２６ａからなることが可能である。非線形スクランブラ２０２は、非線形スクランブラ２０２の出力ビットが長符号マスクのビットに対して非線形に依存するように、長符号配列のビットをスクランブルする。非線形スクランブラ２０２の実施例については後で図９～図１５を参照して説明する。非線形スクランブラ２０２によって生成される非線形性はさまざまなものが可能である。例えば、非線形スクランブラ２０２はフィードバックループを含むことが可能である。あるいは、非線形スクランブラ２０２は、長符号配列に非線形性を導入する簡単な組合せ論理回路からなることも可能である。このようにして、本発明によって構成されるシステムは、盗聴者が長符号マスクＭのビットを取得することに対する困難性を増大させる。デシメータ２０４は、長符号生成器２０２から、既知の周波数を有するビット出力を選択する。例えば、デシメータ２０４は、長符号生成器２０２による６４のビット出力のうち一つを出力しうる。加算器２０

26

６は、デシメータ２０４からの信号とビットインタリーバ１３４からの信号を（２を法として）加える。

【００３４】図8は、１６４において一般的に示された、図６の順方向通信路１６２で用いられる、復号化器の実施例である。復号化器１６４は、長符号マスク生成器２０８、長符号生成器２１０、デシメータ２１２の直列の結合をもって、キー信号を生成する。デシメータ２１２の出力は、モジュロ２の（２を法とする）加算器２１４の第一の入力に結びつけられている。加算器２１４の第二の入力は、ウォルシュ記号変調器１９２に結びつけられている。

【００３５】動作中は、復号化器１６４は、キー信号を生成し、基地局１１２から受信した信号の暗号を復号化する。そのように、復号化器１６４は、暗号化器１３０で生成されたキー信号と同一なキー信号を独立に生成している。そこで、長符号マスク生成器２０８は、固有の長符号マスクからビット配列を生成する。長符号生成器２０８は、長符号配列のビットが長符号マスクのビットに線形に依存するような、図３の長符号生成器２６ａからなることが可能である。非線形スクランブラ２１０は、非線形スクランブラ２１０の出力ビットが長符号マスクのビットに対して非線形に依存するように、長符号配列のビットをスクランブルする。非線形スクランブラ２１０の実施例については後で図９～図１５を参照して説明する。非線形スクランブラ２１０によって生成される非線形性はさまざまなものが可能である。例えば、非線形スクランブラ２１０はフィードバックループを含むことが可能である。あるいは、非線形スクランブラ２１０は、長符号配列に非線形性を導入する簡単な組合せ論理回路からなることも可能である。このようにして、本発明によって構成されるシステムは、盗聴者が長符号マスクＭのビットを取得することに対する困難性を増大させる。デシメータ２１２は、長符号生成器２１０から、既知の周波数を有するビット出力を選択する。例えば、デシメータ２１２は、長符号生成器２１０による６４のビット出力のうち一つを出力しうる。加算器２１４は、デシメータ２１２からの信号とウォルシュ関数復調器１９２からの信号を加える。

【００３６】図9は、２０２ａにおいて一般的に示され、本発明の教示するところに従って構成された、非線形スクランブラの実施例である。注意すべき点であるが、図９～図１５で示された回路は、暗号化器１３０または復号化器１６４のいずれにおいて使用することも可能である。簡単のため、図９～図１５の説明は、暗号化器１３０の場合についてだけ行う。スクランブラ２０２ａは、排他的ＯＲゲート２１６、シフトレジスタ２１８、論理回路２２０およびスイッチ２２２からなる。長符号生成器２００の出力および論理回路２２０の出力は排他的ＯＲゲート２１６の入力に送られる。排他的ＯＲゲート２１６の出力はシフトレジスタ２１８およびスイ

ッチ２２２に接続される。論理回路２２０は、シフトレジスタ２１８の複数のセルへのタップを有する。最後に、長符号生成器２００の出力はスイッチ２２２にも接続される。

【００３７】動作時には、スクランブラ２０２ａは、フィードバックループを用いることにより長符号配列のビットを非線形に組み合わせたビット配列を出力する。排他的ＯＲゲート２１６はビットをシフトレジスタ２１８に出力する。そのビットはシフトレジスタ２１８を通してシフトされ、論理回路２２０で選択的に組み合わされる。論理回路２２０は例えば単純なＡＮＤゲートからなる。あるいは、論理回路２２０は複雑な組合せ論理回路からなることも可能である。論理回路２２０は、シフトレジスタ２１８に入るビットが最終的に、長符号配列の現在のビットと、排他的ＯＲゲート２１６によって出力された過去のビットの論理的組合せとに依存するように、排他的ＯＲゲート２１６への第２の入力を有する。スイッチ２２２は、長符号生成器２００をデシメータ２０４に直接接続することによってスクランブラ２０２ａの効果をバイパスさせることも可能である。シフトレジスタ２１８をクリアするためのリセット信号も設けられる。

【００３８】図１０に、本発明に従って構成された非線形スクランブラのもう一つの実施例２０２ｂを示す。スクランブラ２０２ｂは、６４個のセルを有するシフトレジスタ２２４からなる。シフトレジスタ２２４の各セルはマルチプレクサ２２６の入力に接続される。さらに、シフトレジスタ２２４の０～５とラベルされたセルはマルチプレクサ２２６のセレクタ入力に接続される。注意すべき点であるが、マルチプレクサ２２６のセレクタ入力としては、シフトレジスタ２２４のセルのうちのいずれの６個を使用することも可能である。

【００３９】動作時には、長符号配列のビットはシフトレジスタ２２４を通ってシフトされる。シフトレジスタ２２４のセル０～５内の値は、シフトレジスタ２２４のセルのうちから、マルチプレクサ２２６が出力ビットとしてデシメータ２０４に渡すセルを選択する。

【００４０】図１１に、本発明に従って構成された非線形スクランブラのもう一つの実施例２０２ｃを示す。スクランブラ２０２ｃは、６４個のセルを有するシフトレジスタ２２８からなる。シフトレジスタ２２８のN個の選択されたセルがマルチプレクサ２３０のセレクタ入力に接続される。さらに、シフトレジスタ２２８の２～［N］個の選択されたセルがマルチプレクサ２３０の入力としても接続される。

【００４１】動作時には、長符号配列のビットはシフトレジスタ２２８を通ってシフトされる。マルチプレクサ２３０は、シフトレジスタ２２８からのセレクタ入力に基づいてシフトレジスタ２２８の一つのセルを選択する。選択されたセルの値はスクランブラ２０２ｃの出力としてデシメータ２０４に渡される。

【００４２】図１２に、本発明に従って構成された非線形スクランブラのもう一つの実施例２０２ｄを示す。スクランブラ２０２ｄは、６４個のセルを有するシフトレジスタ２３２からなる。シフトレジスタ２３２の各セルはデータ暗号化規格（ＤＥＳ）回路２３４の入力に接続される。ＤＥＳ回路２３４は、Federal InformationProcessing Standards Publication 46 (January 15, 1977)に従ってデータを暗号化する。秘密鍵信号がＤＥＳ回路２３４に入力される。ＤＥＳ回路２３４は、レジスタ２３６に接続された６４個の出力を有する。レジスタ２３６の選択された一つのセルがスクランブル回路２０２ｄの出力となる。

【００４３】動作時には、長符号配列のビットはシフトレジスタ２３２を通ってシフトされる。ＤＥＳ回路２３４は、鍵信号および通常のＤＥＳ方式を用いてシフトレジスタ２３２内のデータを暗号化する。ＤＥＳ回路２３４は、シフトレジスタ２３２内のデータの暗号化版をレジスタ２３６に出力する。スクランブラ２０２ｄはレジスタ２３６からの出力信号をデシメータ２０４に送る。

【００４４】図１３に、本発明に従って構成された非線形スクランブラのもう一つの実施例２０２ｅを示す。スクランブラ２０２ｅは、６４個のセルを有するシフトレジスタ２４０からなる。シフトレジスタ２４０のN個の選択されたセルが非線形関数要素２４２の入力に接続される。例えば、非線形関数要素２４２は、２個の入力ＡＮＤゲートと、非線形出力を生成するための適当な関数要素とからなる。

【００４５】動作時には、長符号配列のビットはシフトレジスタ２４０を通ってシフトされる。非線形関数要素２４２は、シフトレジスタ２４０のN個の入力セルの値に基づいて出力信号を生成する。

【００４６】図１４に、本発明に従って構成された非線形スクランブラのもう一つの実施例２０２ｆを示す。スクランブラ２０２ｆは、排他的ＯＲゲート２４４、シフトレジスタ２４６、第１論理回路２４８および第２論理回路２５０からなる。長符号生成器２００の出力および第１論理回路２４８の出力は排他的ＯＲゲート２４４の入力に接続される。排他的ＯＲゲート２４４はシフトレジスタ２４６に接続される。第１論理回路２４８はシフトレジスタ２４６の複数のセルへのタップを有する。最後に、第２論理回路２５０は、シフトレジスタ２４６のセルのうちの第２の選択されたセットへのタップを有する。第２論理回路２５０の出力は、スクランブラ２０２ｆの出力となる。シフトレジスタ２４８および２５０をクリアするためのリセット信号も設けられる。

【００４７】動作時には、スクランブラ２０２ｆは、フィードバックループを用いることにより長符号配列のビットを非線形に組み合わせたビット配列を出力する。排他的ＯＲゲート２４４はビットをシフトレジスタ２４６

に出力する。そのビットはシフトレジスタ２４６を通してシフトされ、第１論理回路２４８で選択的に組み合わされる。第１論理回路２４８は例えば単純なＡＮＤゲートからなる。あるいは、第１論理回路２４８は複雑な組合せ論理回路からなることも可能である。第１論理回路２４８は、シフトレジスタ２４６に入るビットが最終的に、長符号配列の現在のビットと、排他的ＯＲゲート２４４によって出力された過去のビットの論理的組合せとに依存するように、排他的ＯＲゲート２４４への第２の入力を有する。第２論理回路２５０は、レジスタ２４６の選択されたセルからのビットを組み合わせてスクランブラ２０２ｆの出力とする。

【００４８】図１５に、本発明に従って構成された非線形スクランブラのもう一つの実施例２０２ｇを示す。スクランブラ２０２ｆは、排他的ＯＲゲート２５２、シフトレジスタ２５４、第１論理回路２５６および第２論理回路２５８からなる。長符号生成器２００の出力および第１論理回路２５６の出力は排他的ＯＲゲート２５２の入力に接続される。排他的ＯＲゲート２５２はシフトレジスタ２５４に接続される。第１論理回路２５６はシフトレジスタ２５６の複数のセルへのタップを有する。さらに、秘密鍵信号Ｋ～｛１｝が、暗号化信号を生成する際に使用するために第１論理回路２５６に入力される。第２論理回路２５８は、シフトレジスタ２５４のセルのうちの第２の選択されたセットへのタップを有する。第２の秘密鍵Ｋ～｛２｝が、暗号化信号を生成する際に使用するために第２論理回路２５８に入力される。第２論理回路２５８の出力は、スクランブラ２０２ｇの出力となる。シフトレジスタ２５６および２５８をクリアするためのリセット信号も設けられる。

【００４９】動作時には、スクランブラ２０２ｇは、秘密のビット配列への非線形依存性を有するビット配列を出力する。この秘密ビット配列としては、長符号生成器２００によって処理された長符号マスク、信号Ｋ～｛１｝もしくはＫ～｛２｝、またはそれらの適当な組合せが可能である。排他的ＯＲゲート２５２はビットをシフトレジスタ２５４に出力する。そのビットはシフトレジスタ２５４を通してシフトされ、第１論理回路２５６で信号Ｋ～｛１｝のビットと選択的に組み合わされる。第１論理回路２５６は例えば単純なＡＮＤゲートからなる。あるいは、第１論理回路２５６は複雑な組合せ論理回路からなることも可能である。第１論理回路２５６は、シフトレジスタ２５４に入るビットが最終的に、長符号配列の現在のビットと、排他的ＯＲゲート２５２によって出力された過去のビットと信号Ｋ～｛１｝の論理的組合せとに依存するように、排他的ＯＲゲート２５２への第２の入力を有する。第２論理回路２５８は、レジスタ２５４の選択されたセルからのビットを信号Ｋ～｛２｝のビットと組み合わせてスクランブラ２０２ｇの出力とする。

【００５０】注意すべき点であるが、非線形スクランブラ２０２ｇは、長符号生成器２００を使用しない従来のシステムよりも強い秘密保護を達成することができる。長符号生成器２００が暗号化器１３０から除かれた場合、秘密性を増大させるためには、Ｋ～｛１｝、Ｋ～｛２｝またはその両方を秘密にしなければならない。さらに、Ｋ～｛１｝、Ｋ～｛２｝またはその両方が秘密である場合、長符号生成器２００は、公開の長符号マスクＭから長符号配列を生成することが可能である。さらに注意すべき点であるが、Ｋ～｛１｝またはＫ～｛２｝のいずれかを省略したものも本発明の技術的範囲内にある。

【００５１】図１６に、図５の基地局１１２で使用するための暗号化器のもう一つの実施例１３０ａを示す。暗号化器１３０ａは、シフトレジスタ２６０、非線形組合せ器２６２およびデシメータ２６４の直列結合によって鍵信号を生成する。デシメータ２６４の出力はモジュロ２加算器２６６の第１入力に接続される。加算器２６６の第２入力はビットインタリーバ１３４に接続される。秘密の長符号マスクＭが非線形組合せ器２６２に入力される。

【００５２】動作時には、暗号化器１３０ａは、長符号マスクのビットの非線形組合せであるビットによって鍵信号を生成する。シフトレジスタ２６０は公知の量からビット配列を生成する。非線形組合せ器２６２は、長符号マスクＭをシフトレジスタ２６０の出力と組み合わせる。デシメータ２６４は、非線形組合せ器２６２から出力されるビットを既知の周期で選択する。例えば、デシメータ２６４は、非線形組合せ器２６２によって出力されるビットを６４個に１個の割合で出力する。加算器２６６は、ビットインタリーバ１３４からの信号をデシメータ２６４からの信号と（２を法として）加算する。

【００５３】図１７に、図６の無線端末１２４で使用するための復号化器のもう一つの実施例１６４ａを示す。復号化器１６４ａは、シフトレジスタ２６８、非線形組合せ器２７０およびデシメータ２７２の直列結合によって鍵信号を生成する。デシメータ２７２の出力はモジュロ２加算器２７４の第１入力に接続される。加算器２７４の第２入力はウォルシュ記号復調器１５４に接続される。秘密の長符号マスクＭが非線形組合せ器２７０に入力される。

【００５４】動作時には、復号化器１６４ａは、長符号マスクのビットの非線形組合せであるビットによって鍵信号を生成する。シフトレジスタ２６８は公知の量からビット配列を生成する。非線形組合せ器２７０は、長符号マスクＭをシフトレジスタ２６８の出力と組み合わせる。デシメータ２７２は、非線形組合せ器２６２から出力されるビットを既知の周期で選択する。例えば、デシメータ２７２は、非線形組合せ器２７０によって出力されるビットを６４個に１個の割合で出力する。加算器２

７４は、ウォルシュ記号復調器１５４からの信号をデシメータ２７２からの信号と（２を法として）加算する。

【００５５】以上、本発明の実施例について詳細に説明したが、以上説明した実施例以外にもさまざまな変形例が可能である。例えば、図９～図１５に示したシフトレジスタは６４セルのものに限定されない。セルの数を変更したものも、本発明の技術的範囲内にある。６４セルのレジスタは単に例示のためのものであり、本発明を限定するものではない。さらに、上記の暗号化器および復号化器はデシメータなしで用いることも可能である。あるいは、デシメータの機能の一部または全部を他の回路に含めることも可能である。

【００５６】スクランブラ２０２ａ～２０２ｇはそれぞれ一つまたは複数のシフトレジスタを有する。強調しておくが、これらのシフトレジスタは単に例示のためのものであり、本発明を限定するものではない。シフトレジスタは、連続する出力ビットを生成する際に使用するためにスクランブラに供給される入力ビットを記憶するものである。この目的で、これと同じ機能を実行するために、図９～図１５のシフトレジスタを適当な回路で置き換えることも可能である。

【００５７】本発明に従って基地局および無線端末内に構成される非線形スクランブラが、伝送中に同一の長符号系列入力を与えられたときに同一の出力を生成することを保証するため、スクランブラは同じ内部状態から始動すべきである。従って、スクランブラ内のシフトレジスタは同一内容で始動しなければならない。これを実現する一つの方法は、ハンドオフ中のリセット信号に応答してシフトレジスタを固定内部値でリセットすることである。図９、図１４および図１５に示したリセット信号は、この機能を実装するために使用可能である。また、レジスタは、各新フレームの最初のようなときにリセットすることも可能である。

【００５８】注意すべき点であるが、図９、図１４および図１５に示した排他的ＯＲゲートは、モジュロ２加算を実行する適当な演算要素により実装することが可能である。

【００５９】また、注意すべき点であるが、長符号マスク中のビット数を４２以外とすることも、本発明の技術的範囲内にある。

【００６０】

【発明の効果】本発明の実施例により、盗聴者の、暗号化された伝送について暗号解析（暗号解読）するという能力を、実質的に排除あるいは減少させることが可能となった。例えば、変化する回転長符号マスクを創り出す長符号マスク生成器を含むことで、長符号配列から線形性を取り除き、長符号マスクを決定することにより、暗号化された出力信号を暗号解析（暗号解読）することを、より困難としたといえる。

【図面の簡単な説明】

【図１】図１は、米国電気通信産業協会(the Telecommunication Industry Association)により、PN-3421として1994年12月に公表された標準案に従った、スペクトル拡散無線通信システムの順方向通信路回路のブロック線図である。

【図２】図２は、図１の順方向通信路回路において用いられる、畳込み符号器のブロック線図である。

【図３】図３は、図１の順方向通信路回路において用いられる、長符号生成器の実施例のブロック線図である。

【図４】図４は、本発明の教示するところに従って構成された、非線形スクランブラを組み込んでいるスペクトル拡散無線インフラストラクチャのブロック線図である。

【図５】図５は、図４のスペクトル拡散無線システムにおける、基地局のブロック線図である。

【図６】図６は、図４のスペクトル拡散無線システムにおける、無線端末のブロック線図である。

【図７】図７は、図５の基地局において用いられる、暗号化器の実施例である。

【図８】図８は、図６の無線端末において用いられる、復号化器の実施例である。

【図９】図９は、図７の暗号化器および図８の復号化器において用いられる、長符号マスク生成器の実施例である。

【図１０】図１０は、図７の暗号化器および図８の復号化器において用いられる、長符号マスク生成器の別の実施例である。

【図１１】図７の暗号化器および図８の復号化器で用いられる非線形スクランブラのもう一つの実施例の図である。

【図１２】図７の暗号化器および図８の復号化器で用いられる非線形スクランブラのもう一つの実施例の図である。

【図１３】図７の暗号化器および図８の復号化器で用いられる非線形スクランブラのもう一つの実施例の図である。

【図１４】図７の暗号化器および図８の復号化器で用いられる非線形スクランブラのもう一つの実施例の図である。

【図１５】図７の暗号化器および図８の復号化器で用いられる非線形スクランブラのもう一つの実施例の図である。

【図１６】図５の基地局で用いられる暗号化器のもう一つの実施例の図である。

【図１７】図６の無線端末で用いられる復号化器のもう一つの実施例の図である。

【符号の説明】

１０　順方向通信路（順方向チャネル）
１２　通信路符号器（チャネル符号器）
１４　ブロックインタリーバ

33

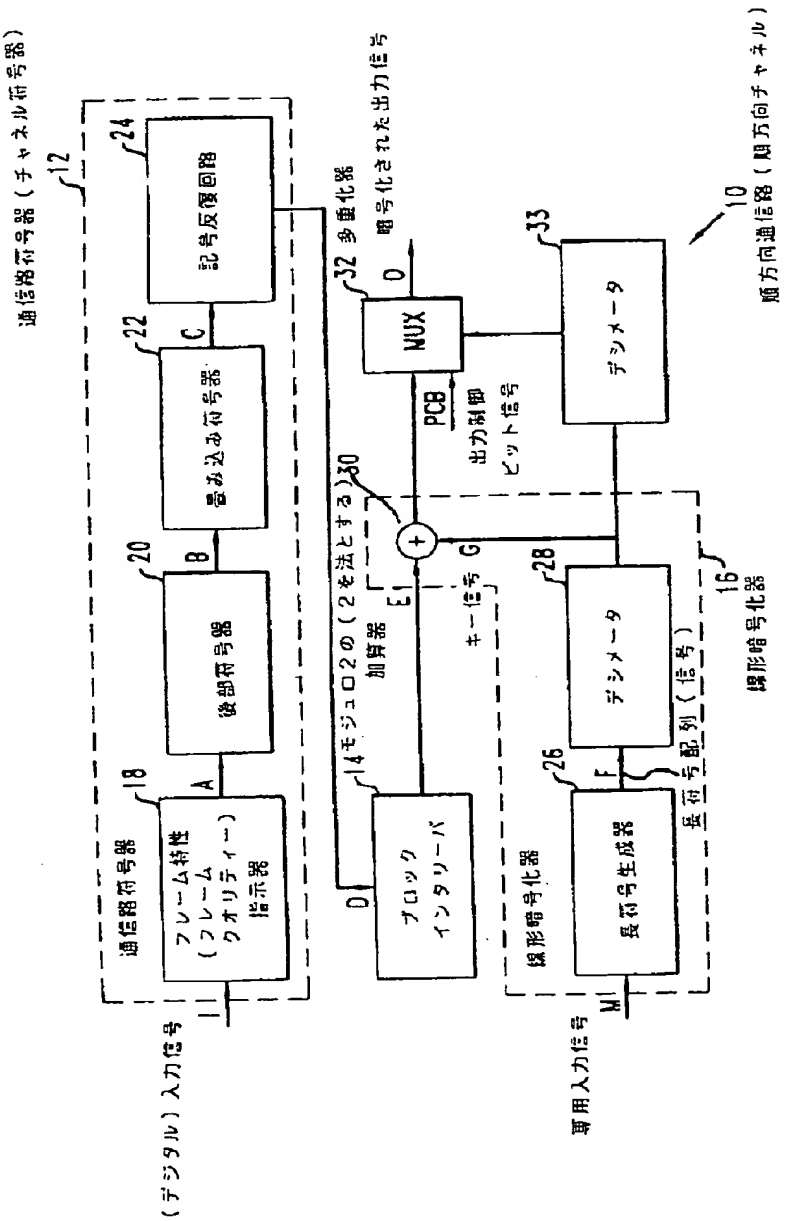
１６　線形暗号化器
１８　フレーム特性（フレームクオリティ）指示器
２０　後部符号器
２２、２２ａ　畳込み符号器
２４　記号反復回路
２６、２６ａ　長符号生成器
２８　デシメータ
３０　モジュロ２の（２を法とする）加算器
３２　多重化器
３３　デシメータ
３４　線形桁送りレジスタ（線形シフトレジスタ）
３４ａ、３４ｂ、３４ｃ、３４ｄ、３５ｅ、３４ｆ、３４ｇ、３４ｈ　ビット位置
３６、３８　モジュロ２の（２を法とする）加算器
３９　インタリーバ
４０　線形フィードバック桁送りレジスタ（線形フィードバックシフトレジスタ）
４２　ＡＮＤゲート
４４　加算器
１１０　無線システム
１１２　基地局
１１４　移動交換局（Mobile Switching Center, ＭＳＣ）
１１６　公衆交換電話回線網（Public Switched Telephone Network, ＰＳＴＮ）
１１８　市内局
１２０　市外局
１２２　固定端末
１２４　無線端末
１２６、１６２　順方向通信路（順方向チャネル）
１２８、１６０　逆監視通信路（リバースチャネル）
１３０　暗号化器
１３２、１７０　通信路符号器（チャネル符号器
１３４、１７２　ビットインタリーバ
１３６、１７４　ウォルシュ関数変調器
１３８、１７８　直角位相拡散器
１４０、１８０　直角位相搬送波変調器
１４２、１８２　ＲＦ送信器
１４４、１８４　アンテナ
１４６、１８６　ＲＦ受信器
１４８、１８８　直角位相搬送波復調器
１５０、１９０　直角位相逆拡散器
１５２　逆拡散器
１５４　ウォルシュ記号復調器
１５６　ビットデインタリーバ
１５８、１９６　通信路復号器（チャネル復号器）

34

１６４　復号化器
１６６　入出力（Ｉ／Ｏ）装置
１６８　音声符号器
１７６　拡散器
１９２　ウォルシュ関数変調器
１９４　ビットデインタリーバ
１９８　音声復号器
２００、２０８　長符号マスク生成器
２０２、２１０　非線形スクランブラ
２０４、２１２　デシメータ
２０６、２１４　モジュロ２の（２を法とする）加算器
２１６　排他的ＯＲゲート
２１８　シフトレジスタ
２２０　論理回路
２２２　スイッチ
２２４　シフトレジスタ
２２６　マルチプレクサ
２２８　シフトレジスタ
２３０　マルチプレクサ
２３２　シフトレジスタ
２３４　データ暗号化規格（ＤＥＳ）回路
２３６　レジスタ
２４０　シフトレジスタ
２４２　非線形関数要素
２４４　排他的ＯＲゲート
２４６　シフトレジスタ
２４８　第１論理回路
２５０　第２論理回路
２５２　排他的ＯＲゲート
２５４　シフトレジスタ
２５６　第１論理回路
２５８　第２論理回路
２６０　シフトレジスタ
２６２　非線形組合せ器
２６４　デシメータ
２６６　モジュロ２加算器
２６８　シフトレジスタ
２７０　非線形組合せ器
２７２　デシメータ
２７４　モジュロ２加算器
Ｉ　（デジタル）入力信号
Ｍ　専用入力信号
Ａ、Ｂ、Ｃ、Ｄ、Ｅ、Ｏ、　信号
Ｆ　長符号配列（信号）
Ｇ　キー信号（鍵信号）

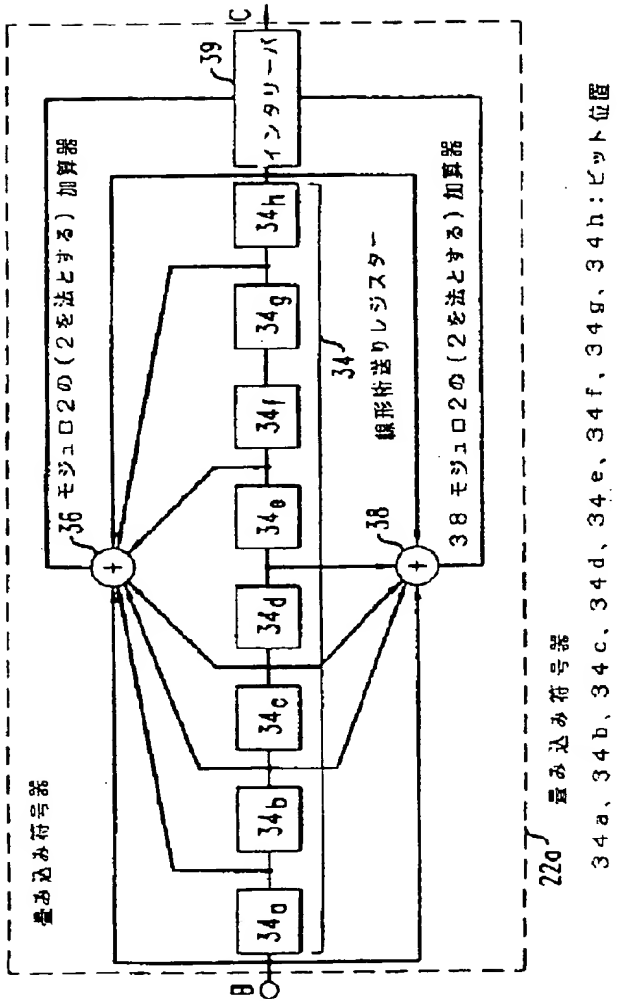
【図1】

（先行技術）


通信路符号器（チャネル符号器）
12
通信路符号器
フレーム特性（フレームクオリティー）指示器
18
A
後部符号器
20
B
畳み込み符号器
22
C
記号反復回路
24
（デジタル）入力信号
I
ブロックインタリーバ
14
モジュロ2の（2を法とする）加算器
30
D
E1
キー信号
G
多重化器
32
MUX
D
暗号化された出力信号
PCB
出力制御ビット信号
デシメータ
33
10
順方向通信路（順方向チャネル）
線形暗号化器
長符号生成器
26
F
デシメータ
28
長符号配列（信号）
線形暗号化器
16
専用入力信号
M

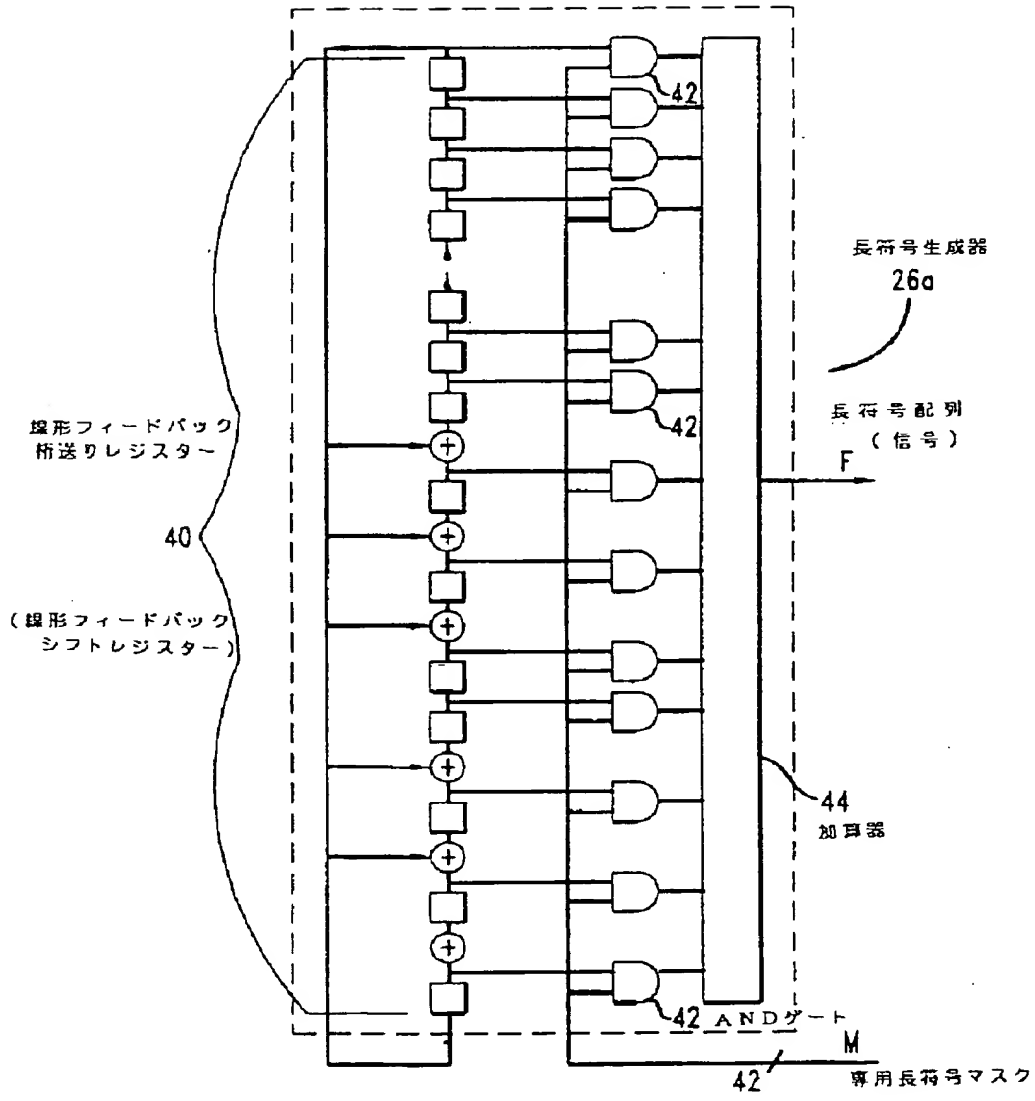
【図2】

（先行技術）

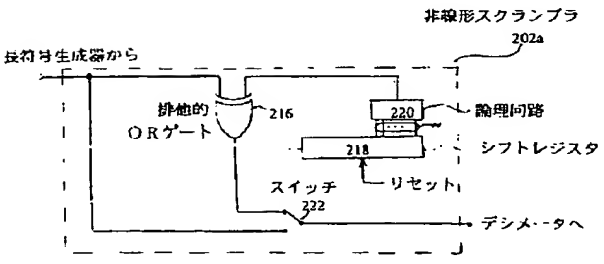

IC
39
インタリーバ
34h
34g
34f
34e
34d
34c
34b
34a
34
線形帰還レジスタ
36 モジュロ2の（2を法とする）加算器
38 モジュロ2の（2を法とする）加算器
38
B
220
畳み込み符号器
34a、34b、34c、34d、34e、34f、34g、34h：ビット位置

【図3】

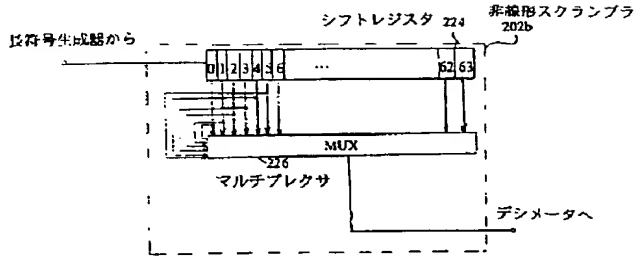
（先行技術）



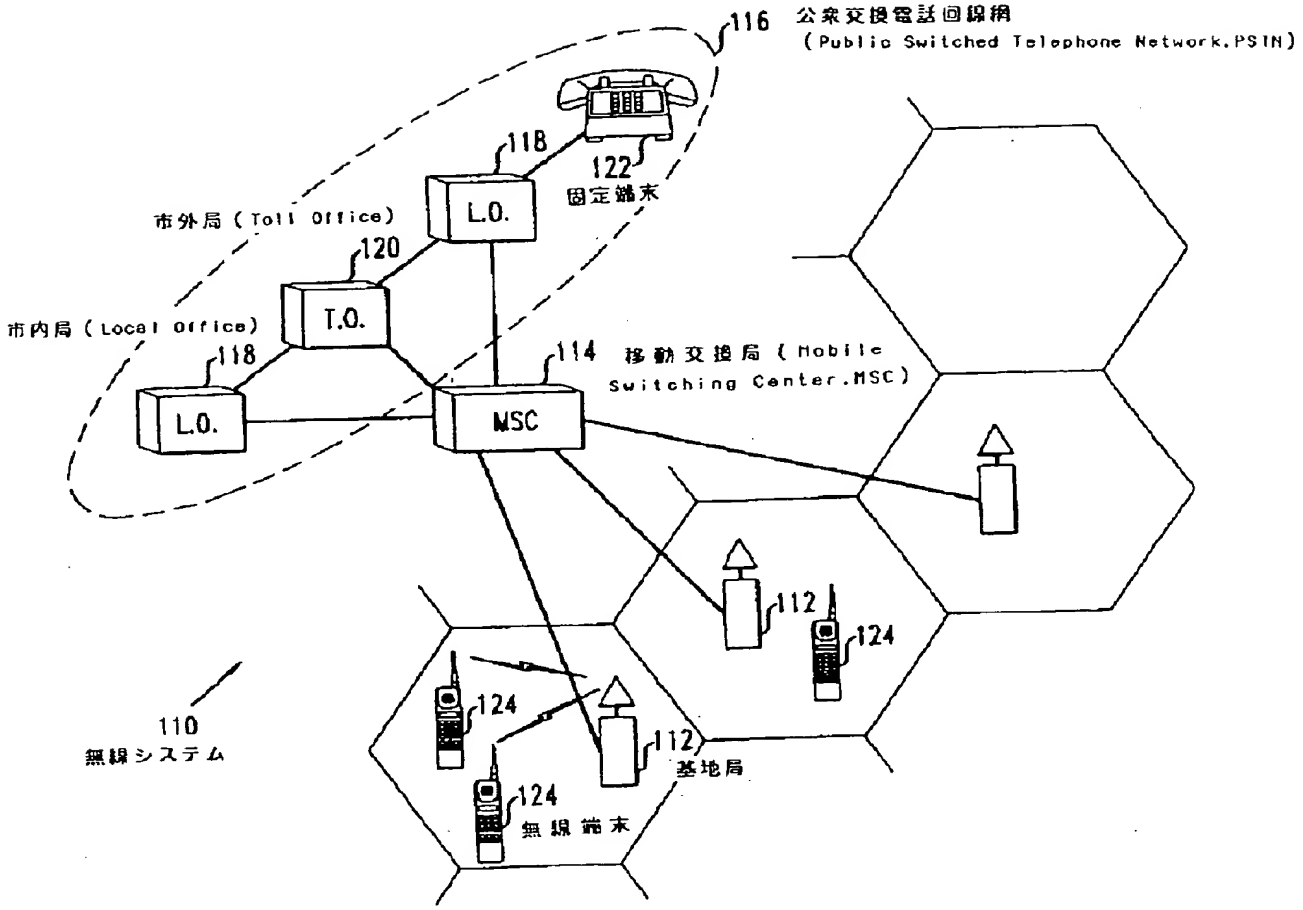
【図9】



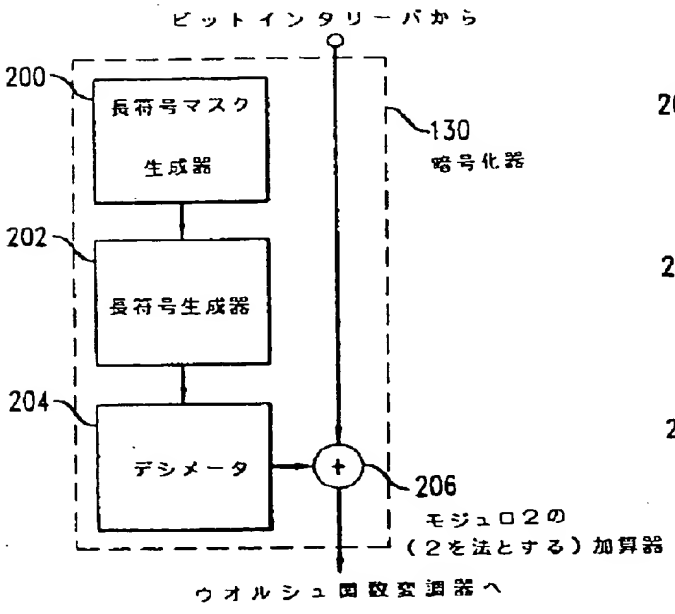
【図10】



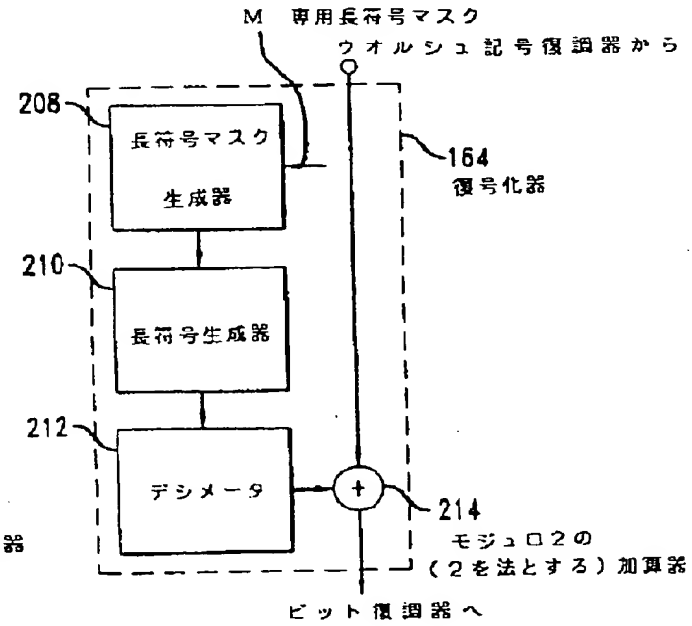
【図4】


116
公衆交換電話回線網
(Public Switched Telephone Network.PSIN)
118
122
固定端末
L.O.
市外局 (Toll Office)
120
T.O.
市内局 (Local Office)
118
L.O.
114
移動交換局 (Mobile Switching Center.MSC)
MSC
112
124
124
112
基地局
124
無線端末
110
無線システム

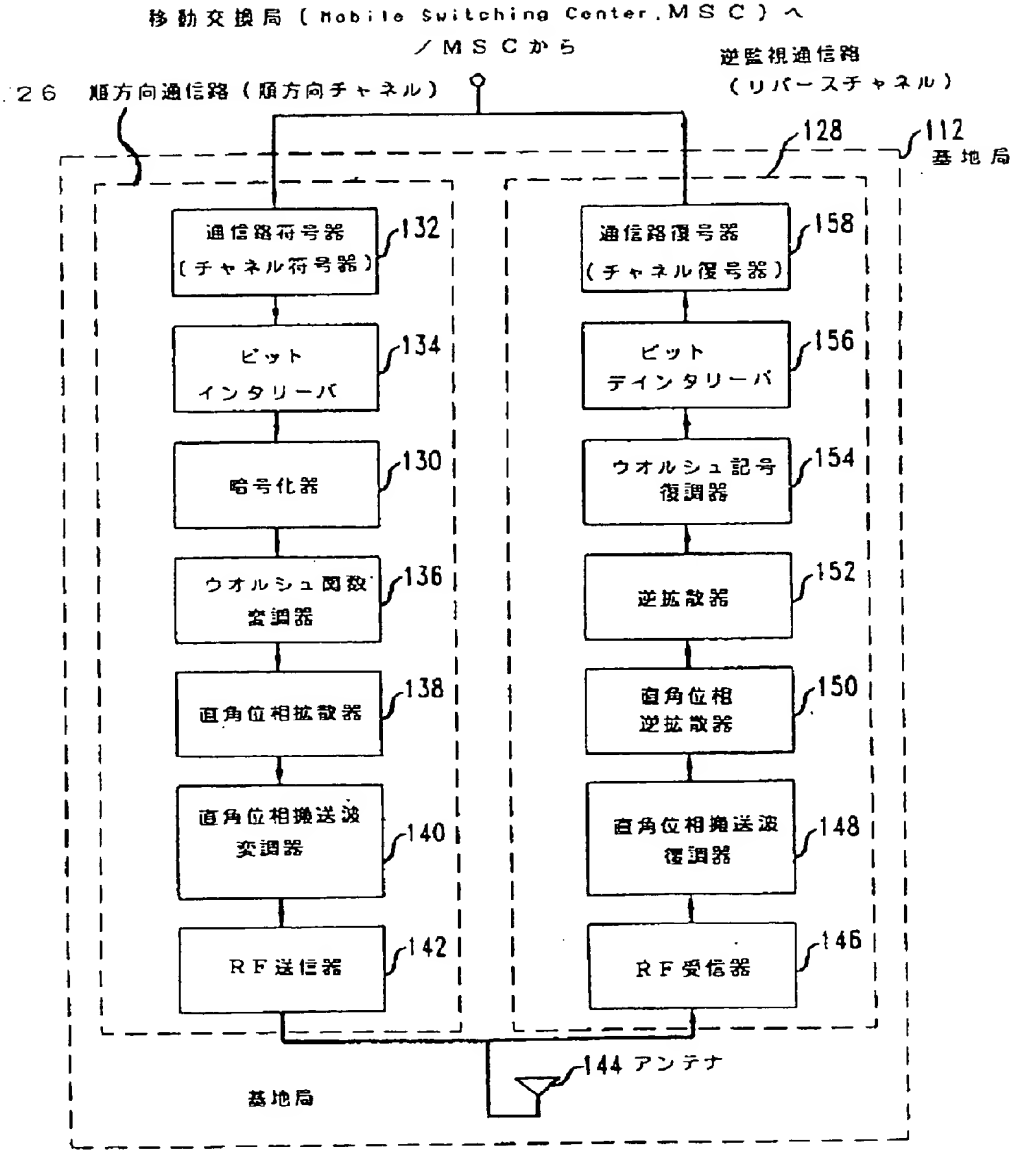
【図7】


ビットインタリーバから
200
長符号マスク生成器
130
暗号化器
202
長符号生成器
204
デシメータ
206
モジュロ2の(2を法とする)加算器
ウォルシュ関数変調器へ

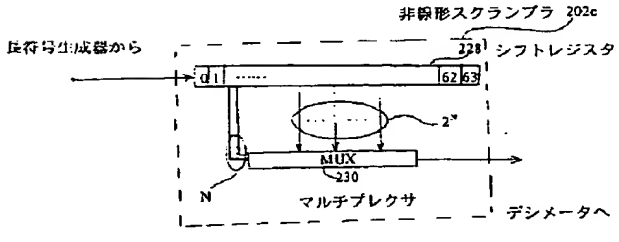
【図8】


M 専用長符号マスク
ウォルシュ記号復調器から
208
長符号マスク生成器
164
復号化器
210
長符号生成器
212
デシメータ
214
モジュロ2の(2を法とする)加算器
ビット復調器へ

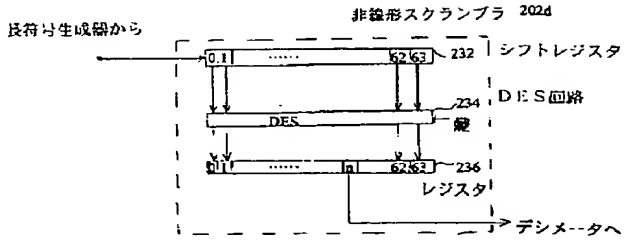
【図5】


移動交換局（Mobile Switching Center，ＭＳＣ）へ
／ＭＳＣから
逆監視通信路
（リバースチャネル）
順方向通信路（順方向チャネル）
126
128
112
基地局
通信路符号器
（チャネル符号器）
132
ビット
インタリーバ
134
暗号化器
130
ウオルシュ関数
変調器
136
直角位相拡散器
138
直角位相搬送波
変調器
140
ＲＦ送信器
142
通信路復号器
（チャネル復号器）
158
ビット
デインタリーバ
156
ウオルシュ記号
復調器
154
逆拡散器
152
直角位相
逆拡散器
150
直角位相搬送波
復調器
148
ＲＦ受信器
146
144 アンテナ
基地局

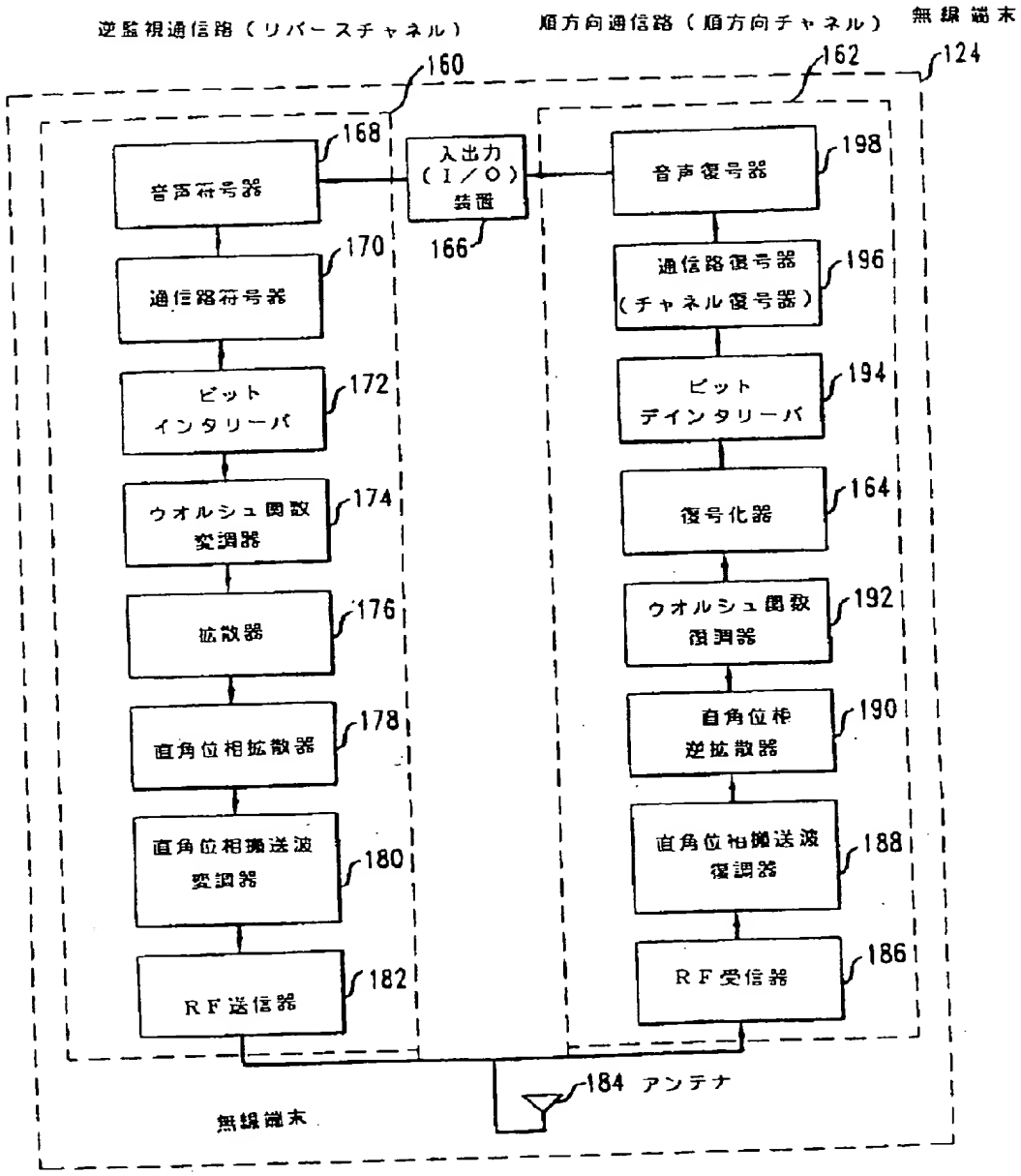
【図11】


非線形スクランブラ 202c
長符号生成器から
228
シフトレジスタ
MUX
230
N
マルチプレクサ
デシメータへ

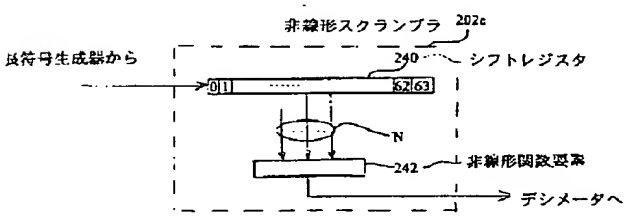
【図12】


非線形スクランブラ 202d
長符号生成器から
232
シフトレジスタ
DES回路
234
鍵
DES
236
レジスタ
デシメータへ

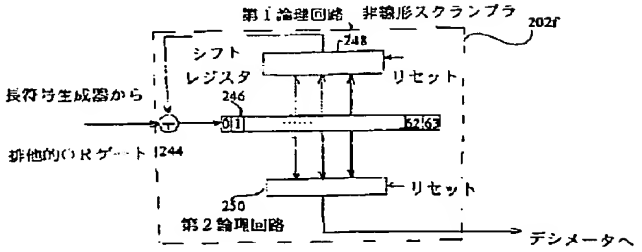
【図6】


逆監視通信路（リバースチャネル）
順方向通信路（順方向チャネル）
無線端末
160
162
124
168
音声符号器
入出力（I／O）装置
166
音声復号器
198
170
通信路符号器
通信路復号器（チャネル復号器）
196
172
ビットインタリーバ
ビットデインタリーバ
194
174
ウオルシュ関数変調器
復号化器
164
176
拡散器
ウオルシュ関数復調器
192
178
直角位相拡散器
直角位相逆拡散器
190
180
直角位相搬送波変調器
直角位相搬送波復調器
188
182
RF送信器
RF受信器
186
184 アンテナ
無線端末

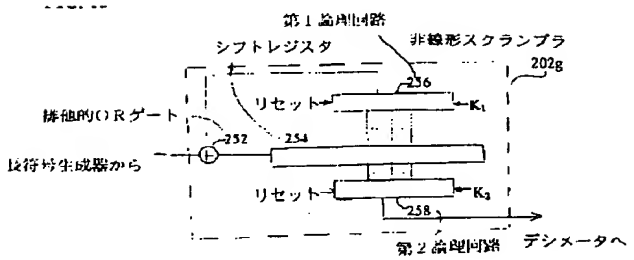
【図13】


非線形スクランブラ
202e
長符号生成器から
240
シフトレジスタ
0 1
62 63
N
242
非線形関数要素
デシメータへ

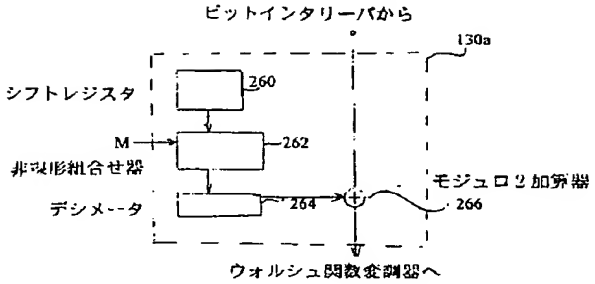
【図14】


第1論理回路
非線形スクランブラ
202f
248
シフトレジスタ
リセット
長符号生成器から
246
0 1
62 63
非他的ORゲート
244
リセット
250
第2論理回路
デシメータへ

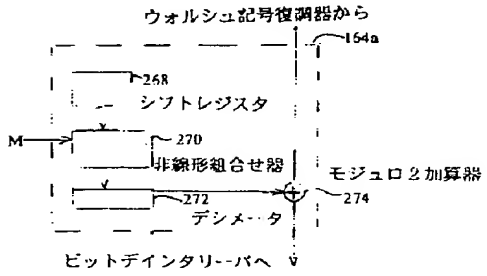
【図１５】



【図１６】



【図１７】



フロントページの続き

(51) Int. Cl. ⁶	識別記号	庁内整理番号	Ｆ Ｉ	技術表示箇所
9/20			653	

【外国語明細書】

1. Title of Invention

CRYPTOGRAPHIC SYSTEM FOR WIRELESS COMMUNICATIONS

2. Claims

1. A base station in a spread spectrum wireless communications system, comprising:

an RF antenna;

a reverse channel that receives and processes a signal from a wireless terminal; and

a forward channel that transmits an input signal from a mobile switching center to a wireless terminal, said forward channel circuit comprising:

a channel coder responsive to said mobile switching center that provides error correction to said input signal,

a bit interleaver responsive to said channel coder that rearranges the order of the bits in the input signal so as to minimize the effect of error bursts,

an encryptor responsive to said channel coder that encrypts said input signal, said encryptor including a nonlinear scrambler for generating a key signal comprising a sequence of bits that have a nonlinear relationship to a private long code mask, and

circuitry responsive to said channel coder, said bit interleaver and said encryptor and coupled to said antenna for modulating and transmitting said input signal.

2. The base station of claim 1, wherein said encryptor comprises:

a long code generator that creates a long code sequence from a long code mask;

a nonlinear scrambler responsive to said long code generator that creates a key signal that is a nonlinear function of the bits of the long code mask; and

a circuit responsive to said bit interleaver and said nonlinear scrambler that encrypts said input signal.

3. The base station of claim 2, wherein said non-linear scrambler comprises:

a shift register having a first predetermined number of cells, said shift register having an input to receive a stream of input bits from said long code register;

a first logic circuit coupled to said shift register so as to access the contents of selected cells, said first logic circuit having an output;

a second logic circuit having first and second inputs and an output, said first input coupled to said long code generator, said second input coupled to said output of said first logic circuit, and said output coupled to said input of said shift register so as to provide a feedback loop for said nonlinear scrambler, said output of said second logic circuit also comprising the output of said nonlinear scrambler.

4. The base station of claim 3, wherein said second logic circuit comprises an Exclusive-OR gate.

5. The base station of claim 2, wherein said nonlinear scrambler includes a feedback loop.

6. The base station of claim 2 wherein said nonlinear scrambler comprises a feedback loop such that an output bit of said nonlinear scrambler is used to create a subsequent output bit.

7. The base station of claim 2, wherein said nonlinear scrambler comprises:

a shift register having a predetermined number of cells, said shift register having an input to receive a stream of input bits from said long code generator; and

a combinational logic circuit coupled to tap the contents of selected cells of said shift register so as to provide an output for said nonlinear scrambler.

8. The base station of claim 7, wherein said combinational logic circuit comprises an AND-gate having at least two inputs coupled to selected cells of said shift register.

9. The base station of claim 2, wherein said nonlinear scrambler comprises:

a shift register having a predetermined number of cells, said shift register having an input to receive a stream of input bits from said long code generator; and

a multiplexer having a predetermined number of data inputs and a predetermined number of selector inputs, said selector inputs coupled to a first set of selected cells of said shift register and said data inputs coupled to a second selected set of cells of said shift register such that the first set of cells selects among the second set of cells to provide an output from said multiplexer.

10. The base station of claim 9, wherein said first and second sets of cells are mutually exclusive.

11. The base station of claim 9, wherein said first and second sets of cells share a predetermined number of cells.

12. The base station of claim 2, wherein said nonlinear scrambler comprises:

a shift register having a predetermined number of cells, said shift register having an input to receive a stream of input bits from said long code generator;

a data encryption standard circuit having a predetermined number of inputs coupled to selected cells of said shift register for using a key signal to create an encrypted output bit for each input; and

a register having a predetermined number of cells, each cell coupled to receive a bit output by said data encryption standard circuit, a selected cell of said register providing the output of said nonlinear scrambling register.

13. The base station of claim 2, wherein said nonlinear scrambler comprises:

a feedback circuit responsive to said long code generator, said feedback circuit including a shift register; and

a combinational logic circuit coupled to tap selected cells of said shift register so as to generate an output for said nonlinear scrambler.

14. An encryptor for encrypting an input signal in a forward channel of a spread spectrum wireless communication system, said encryptor comprising:

a long code generator that creates a long code sequence from a long code mask;

a nonlinear scrambler responsive to said long code generator that creates a key signal that is a nonlinear function of the bits of the long code mask; and

a combinational logic circuit that encrypts said input signal with said key signal.

15. The encryptor of claim 14, wherein said non-linear scrambling circuit comprises:

a shift register having a first predetermined number of cells, said shift register having an input to receive a stream of input bits from said long code register;

a first logic circuit coupled to said shift register so as to access the contents of predetermined cells, said first logic circuit having an output;

a second logic circuit having first and second inputs and an output, said first input coupled to said long code generator, said second input coupled to said output of said first logic circuit, and said output coupled to said input of said shift register so as to provide a feedback loop for said nonlinear scrambler, said output of said second logic circuit also comprising the output of said nonlinear scrambler.

16. The encryptor of claim 15, wherein said second logic circuit comprises an Exclusive-OR gate.

17. The encryptor of claim 14, wherein said nonlinear scrambler comprises a feedback loop such that an output bit of said nonlinear scrambler is used to create a subsequent output bit.

18. The encryptor of claim 14, wherein said nonlinear scrambler comprises:

a shift register having a predetermined number of cells, said shift register having an input to receive a stream of input bits from said long code generator; and

a combinational logic circuit coupled to tap the contents of a predetermined number of said cells of said shift register so as to provide an output of said nonlinear scrambler.

19. The encryptor of claim 18, wherein said combinational logic circuit comprises an AND-gate having at least two inputs coupled to selected cells of said shift register.

20. The encryptor of claim 14, wherein said nonlinear scrambler comprises:

a shift register having a predetermined number of cells, said shift register having an input to receive a stream of input bits from said long code generator; and

a multiplexer having a predetermined number of data inputs and a predetermined number of selector inputs, said selector inputs coupled to a first set of selected cells of said shift register and said data inputs coupled to a second selected set of cells of said shift register such that the first set of cells selects among the second set of cells to provide an output from said multiplexer.

21. The base station of claim 20, wherein said first and second sets of cells are mutually exclusive.

22. The base station of claim 20, wherein said first and second sets of cells share a predetermined number of cells.

23. The base station of claim 14, wherein said nonlinear scrambler comprises:

a shift register having a predetermined number of cells, said shift register having an input to receive a stream of input bits from said long code generator;

a data encryption standard circuit having a predetermined number of inputs coupled to selected cells of said shift register for using a key signal to create an encrypted output bit for each input; and

a register having a predetermined number of cells, each cell coupled to receive a bit output by said data encryption standard circuit, a selected cell of said register providing the output of said nonlinear scrambling register.

24. A wireless terminal for a spread spectrum wireless communication system, comprising:

an RF antenna;

a reverse channel circuit that processes and transmits a signal to a base station; and

a forward channel circuit that receives and processes a transmitted signal from a base station, said forward channel circuit comprising:

a receiver circuit coupled to said antenna that demodulates said transmitted signal,

a decryptor responsive to said receiver circuit that decrypts said transmitted signal, said decryptor including a nonlinear scrambler for generating a key signal comprising a sequence of bits that have a nonlinear relationship to a private long code mask,

a bit deinterleaver responsive to said receiver circuit that rearranges the order of the bits in the transmitted signal,

a channel decoder responsive to said receiver circuit that provides error correction to said transmitted signal,

a voice decoder responsive to said receiver circuit that generates an output signal from said transmitted signal, and

an output device for outputting the transmitted signal.

25. The wireless terminal of claim 24, wherein said decryptor comprises:

a long code generator that creates a long code sequence from a long code mask;

a nonlinear scrambler responsive to said long code generator that creates an key signal that is a nonlinear function of the bits of the long code mask; and

a combinational logic circuit responsive to said nonlinear scrambler and said receiver circuit that decrypts said transmitted signal.

26. The wireless terminal of claim 25, wherein said non-linear scrambling circuit comprises:

a shift register having a first predetermined number of cells, said shift register having an input to receive a stream of input bits from said long code register;

a first logic circuit coupled to said shift register so as to access the contents of selected cells, said first logic circuit having an output;

a second logic circuit having first and second inputs and an output, said first input coupled to said long code generator, said second input coupled to said output of said first logic circuit, and said output coupled to said input of said shift register so as to provide a feedback loop for said nonlinear scrambler, said output of said second logic circuit also comprising the output of said nonlinear scrambler.

27. The wireless terminal of claim 26, wherein said second logic circuit comprises an Exclusive-OR gate.

28. The wireless terminal of claim 25, wherein said nonlinear scrambler includes a feedback loop.

29. The wireless terminal of claim 25 wherein said nonlinear scrambler comprises a feedback loop such that an output bit of said nonlinear scrambler is used to create a subsequent output bit.

30. The wireless terminal of claim 25, wherein said nonlinear scrambler comprises:

a shift register having a predetermined number of cells, said shift register having an input to receive a stream of input bits from said long code generator; and

a combinational logic circuit coupled to tap the contents of selected cells of said shift register so as to provide an output of said nonlinear scrambler.

31. The wireless terminal of claim 30, wherein said combinational logic circuit comprises an AND-gate having at least two inputs coupled to selected cells of said shift register.

32. The wireless terminal of claim 25, wherein said nonlinear scrambler comprises:

a shift register having a predetermined number of cells, said shift register having an input to receive a stream of input bits from said long code generator; and

a multiplexer having a predetermined number of data inputs and a predetermined number of selector inputs, said selector inputs coupled to a first set of selected cells of said shift register and said data inputs coupled to a second selected set of cells of said shift register such that the first set of cells selects among the second set of cells to provide an output from said multiplexer.

33. The wireless terminal of claim 32, wherein said first and second sets of cells are mutually exclusive.

34. The wireless terminal of claim 32, wherein said first and second sets of cells share a predetermined number of cells.

35. The wireless terminal of claim 25, wherein said nonlinear scrambler comprises:

a shift register having a predetermined number of cells, said shift register having an input to receive a stream of input bits from said long code generator;

a data encryption standard circuit having a predetermined number of inputs coupled to selected cells of said shift register for using a key signal to create an encrypted output bit for each input; and

a register having a predetermined number of cells, each cell coupled to receive a bit output by said data encryption standard circuit, a selected cell of said register providing the output of said nonlinear scrambling register.

36. The wireless terminal of claim 25, wherein said nonlinear scrambler comprises:

a feedback circuit responsive to said long code generator, said feedback circuit including a shift register; and

a combinational logic circuit coupled to tap selected cells of said shift register so as to generate an output for said nonlinear scrambler.

37. A method for preventing interception of an information signal from a spread spectrum base station to a wireless terminal in a wireless communications system, said method comprising the steps of:

receiving an input signal from a mobile switching center;

coding said input signal with a channel coder for providing error correction to said input signal;

interleaving the bits of said input signal with a bit interleaver so as to minimize the effect of error bursts;

generating a key signal with an encryptor including a nonlinear scrambler such that the bits of the key signal comprise a sequence of bits that have a nonlinear relationship to a private long code mask;

encrypting said input signal with said key signal;

modulating said input signal for transmission; and

transmitting said input signal.

38. The method of claim 37 wherein said step of generating a key signal comprises the steps of:

generating a long code sequence from a long code mask in a long code generator; and

scrambling said long code sequence in a nonlinear scrambler.

39. The method of claim 38 wherein said step of scrambling the long code sequence comprises the step of scrambling the long code sequence in a nonlinear scrambler having a feedback loop.

40. The method of claim 38 wherein said step of scrambling the long code sequence comprises the step of scrambling the long code sequence in a nonlinear scrambler having a shift register coupled to receive the long code sequence and a combinational logic circuit coupled to selected cells of the shift register to generate the output of the nonlinear scrambler.

41. The method of claim 38 wherein said step of scrambling the long code sequence comprises the steps of:

shifting the bits of the long code sequence through a shift register having a predetermined number of cells; and

using selected cells of said shift register to select among the cells of the shift register to provide an output of said nonlinear scrambler.

42. The method of claim 38 wherein said step of scrambling the long code sequence comprises the steps of:

shifting the bits of the long code sequence through a shift register having a predetermined number of cells; and

encrypting the bits in said shift register with a data encryption standard circuit and a second key signal.

43. A spread spectrum wireless infrastructure, comprising:

a mobile switching center coupled to receive input signals from at least one local office and at least one toll office;

a plurality of base stations coupled to said mobile switching center, each base station comprising:

an RF antenna;

a reverse channel that receives and processes a signal from a wireless terminal; and

a forward channel that transmits an input signal from one of said mobile switching centers to a wireless terminal, said forward channel circuit comprising:

a channel coder responsive to said mobile switching center that provides error correction to said input signal,

a bit interleaver responsive to said channel coder that rearranges the order of the bits in the input signal so as to minimize the effect of error bursts,

an encryptor responsive to said channel coder that encrypts said input signal, said encryptor including a nonlinear scrambler for generating a key signal comprising a sequence of bits that have a nonlinear relationship to a private long code mask, and

circuitry responsive to said channel coder and coupled to said antenna that modulates said input signal.

44. The wireless infrastructure of claim 43, wherein said encryptor comprises:

a long code generator for creating a long code sequence from a long code mask;

a nonlinear scrambler responsive to said long code generator for creating a key signal that is a nonlinear function of the bits of the long code mask; and

a combinational logic circuit responsive to said bit interleaver for encrypting said input signal.

45. The wireless infrastructure of claim 44, wherein said non-linear scrambler comprises:

a shift register having a first predetermined number of cells, said shift register having an input to receive a stream of input bits from said long code register;

a first logic circuit coupled to said shift register so as to access the contents of selected cells, said first logic circuit having an output;

a second logic circuit having first and second inputs and an output, said first input coupled to said long code generator, said second input coupled to said output of said first logic circuit, and said output coupled to said input of said shift register so as to provide a feedback loop for said nonlinear scrambler, said output of said

second logic circuit also comprising the output of said nonlinear scrambler.

46. The wireless infrastructure of claim 45, wherein said second logic circuit comprises an Exclusive-OR gate.

47. The wireless infrastructure of claim 44, wherein said nonlinear scrambler includes a feedback loop.

48. The wireless infrastructure of claim 44 wherein said nonlinear scrambler comprises a feedback loop such that an output bit of said nonlinear scrambler is used to create a subsequent output bit.

49. The wireless infrastructure of claim 44, wherein said nonlinear scrambler comprises:

a shift register having a predetermined number of cells, said shift register having an input to receive a stream of input bits from said long code generator; and

a combinational logic circuit coupled to tap the contents of selected cells of said shift register so as to provide an output of said nonlinear scrambler.

50. The wireless infrastructure of claim 49, wherein said combinational logic circuit comprises an AND-gate having at least two inputs coupled to selected cells of said shift register.

51. The wireless infrastructure of claim 44, wherein said nonlinear scrambler comprises:

a shift register having a predetermined number of cells, said shift register having an input to receive a stream of input bits from said long code generator; and

a multiplexer having a predetermined number of data inputs and a predetermined number of selector inputs, said selector inputs coupled to a first set of selected cells of said shift register and said data inputs coupled to a second selected set of cells of said shift

register such that the first set of cells selects among the second set of cells to provide an output from said multiplexer.

52. The wireless infrastructure of claim 51, wherein said first and second sets of cells are mutually exclusive.

53. The wireless infrastructure of claim 51, wherein said first and second sets of cells share a predetermined number of cells.

54. The wireless infrastructure of claim 44, wherein said nonlinear scrambler comprises:

a shift register having a predetermined number of cells, said shift register having an input to receive a stream of input bits from said long code generator;

a data encryption standard circuit having a predetermined number of inputs coupled to selected cells of said shift register for using a key signal to create an encrypted output bit for each input; and

a register having a predetermined number of cells, each cell coupled to receive a bit output by said data encryption standard circuit, a selected cell of said register providing the output of said nonlinear scrambling register.

55. The wireless infrastructure of claim 44, wherein said nonlinear scrambler comprises:

a feedback circuit responsive to said long code generator, said feedback circuit including a shift register; and

a combinational logic circuit coupled to tap selected cells of said shift register so as to generate an output for said nonlinear scrambler.

3. Detailed Description of Invention

Field of the Invention

This invention relates in general to the field of communications. More particularly, this invention relates to a cryptographic system for wireless communications.

Background of the Invention

Every day, millions of users communicate with wireless systems. Such communications include voice and data transmissions. Most, if not all, users of these systems do not want the content of the communication to be publicly available. Rather, users generally desire to keep the content of the communication private. Unfortunately, without proper cryptographic precautions, interlopers can easily eavesdrop on communications in some wireless systems. For example, most analog wireless systems do not protect communications from interception. An eavesdropper can access the substance of the transmission by simply tuning a radio to the proper frequency.

Some current digital wireless communication systems take precautions to protect the privacy of users. For example, the Telecommunications Industry Association is drafting a standard for a spread spectrum wireless communications system. The current version of the draft standard was published in December of 1994 as *Mobile Station -- Base Station Compatibility Standard for Dual --Mode Spread Spectrum Cellular System* marked *PN-3421 (to be published as IS-95a)* (hereinafter the "Draft Standard") the teachings of which are incorporated herein by reference. The spread spectrum system described in the Draft Standard is referred to colloquially as Code Division Multiple Access, or CDMA. The Draft Standard includes plans for encrypting voice or data signals prior to transmission for added privacy. Thus, only the true recipient of the voice or data transmission should obtain the content of the transmission.

Summary of the Invention

A previously unrecognized problem with the cryptographic system that is specified by the Draft Standard is that it permits an eavesdropper to easily and quickly cryptanalyze transmissions encrypted according to the Draft Standard and thereby gain access to the substance of the transmission. The forward traffic channel described in the Draft Standard calls for encrypting an input voice or data signal prior to transmission with a key signal. The Draft Standard also specifies that the input signal be combined with the

long code sequence in an Exclusive-OR (i.e. mod 2 addition) function to produce an encrypted output signal.

The Draft Standard calls for generating the long code sequence from a publicly known sequence and a private 42-bit pattern, known as the long code mask. The publicly available sequence is placed in what can be conceptualized as a linear shift register. The output of the linear shift register is combined with the bits of the long code mask. The linear nature of the combination causes the long code sequence to depend linearly on the bits of the private long code mask. This enables an eavesdropper to decrypt a wireless communication with access to 42 bits of the long code sequence. The eavesdropper could use the bits from the long code sequence to create 42 linear equations that depend on the 42 unknown bits of the long code mask. However, the Draft Standard does not call for direct transmission of the bits of the long code sequence. Rather, an Exclusive-OR function combines the bits of the long code sequence with the unknown input signal thus corrupting the bits of the long code sequence. This should diminish the chances that an eavesdropper will successfully cryptanalyze a transmission. This is not the case with the Draft Standard because of the way that the input signal is processed to form frames of 384 bits for error correction.

An eavesdropper can cryptanalyze a transmission by recognizing relationships among the last sixteen bits in each frame of the input signal. Specifically, the eavesdropper can combine selected bits of the input signal from the last sixteen bits in each frame so as to produce modulo-2 sums of zero. By adding (mod 2) the bits of the output signal such that the sum of the corresponding input bits is zero, the eavesdropper can obtain data that represent combinations of bits of the long code sequence. Essentially, the eavesdropper can cancel the effect of the input signal on the output signal. Each bit of the long code sequence is linearly dependent on the 42 bits of the long code mask. Thus, the eavesdropper can combine known bits of the output signal to create equations that are linearly dependent on the bits of the long code mask. Successive frames of data yield 42 equations so as to allow decryption of the communication within less than a second after the communication commences.

Embodiments of the present invention substantially eliminate or reduce the ability of eavesdroppers to cryptanalyze encrypted transmissions. Specifically, exemplary embodiments of the present invention include a nonlinear scrambler coupled to the output of the long code generator. This removes the linearity from the decimated long code sequence and makes it more difficult to determine the long code mask and thus cryptanalyze the encrypted output signal.

Detailed Description

The Telecommunications Industry Association (TIA) sets standards for wireless communications systems. The TIA drafted a standard for a spread spectrum wireless communications system. The system described in the draft standard is referred to as Code Division Multiple Access (CDMA). Part of the draft standard addresses the need for privacy in wireless communications. The current version of the draft standard was published in December of 1994 as *Mobile Station -- Base Station Compatibility Standard for Dual --Mode Spread Spectrum Cellular System* marked *PN-3421 (to be published as IS-95a)* (hereinafter the "Draft Standard") the teachings of which are incorporated herein by reference. Upon detailed analysis of the Draft Standard as outlined below, I discovered that a communication system built in compliance with the Draft Standard is prone to attack by eavesdroppers despite the encryption procedure because of previously unknown weaknesses in the design of the cryptosystem. Embodiments of the present invention can overcome this weakness in the encryption procedure of the Draft Standard by providing a forward channel circuit and method with added security for encrypted communications.

A detailed examination of the forward channel circuit specified in the Draft Standard provides an understanding of the weakness of the present cryptographic system. FIGURE 1 is a block diagram of the forward channel circuit indicated generally at 10 in a base station according to the Draft Standard. Forward channel circuit 10 typically comprises channel coder 12, block interleaver 14 and linear encryptor 16.

Channel coder 12 processes a digital input signal, *I*. Input signal *I* may comprise, for example, an encoded digital voice, data or other appropriate signal for transmission in a wireless network. Channel coder 12 and block interleaver 14 minimize the impact on the output of forward channel circuit 10 when consecutive bits of signal *I* are lost or flipped during transmission. Channel coder 12 typically includes the series combination of frame quality indicator 18, tail encoder 20, convolutional encoder 22, and symbol repetition circuit 24. Channel coder 12, together with block interleaver 14, outputs a processed signal *E*.

Linear encryptor 16 producesa key signal *G* to encrypt processed signal *E*. Linear encryptor 16 typically comprises the series combination of long code generator 26

with decimator 28. Long code generator 26 generates a sequence of bits from a private input signal *M* referred to as the long code mask. Signal *F*, output by long code generator 26, is called the long code sequence. Decimator circuit 28 outputs 1 in 64 of the bits of the long code sequence as signal *G*. The output of decimator 28 is coupled to an input of a modulo-2 adder 30 such as an Exclusive-OR function. Channel coder 12 is also coupled to an input of modulo-2 adder 30. Modulo-2 adder 30 outputs an encrypted version of signal *E* to a multiplexer 32. A power control bit signal *PCB* is also provided to multiplexer 32. Multiplexer 32 outputs a signal *O* as the output of forward channel circuit 10 of FIGURE 1. A decimator 33 is coupled between decimator 28 and a control input of multiplexer 32.

In operation, forward channel circuit 10 receives and processes input signal *I* to provide an encrypted output signal *O* for transmission. Input signal *I* is received in frames of bits. The number of bits in each frame may vary based on the information contained in input signal *I*. For example, each frame in the full data rate case includes 172 bits whereas in the lowest data rate case, each frame includes only 16 bits. Symbol repetition circuit 24 replicates the output of convolutional encoder 22 such that the total number of bits in signal *E* in each data rate case is the same. To aid in the analysis below, signals *E*, *G*, and *O* are regarded as binary vectors of length 384 bits. Also, each vector has two subscripts. The first subscript, *f*, refers to the frame of data in producing the vector and the second subscript, *j*, refers to an element or bit of the vector.

Channel coder 12 manipulates input signal *I* to reduce the effect of burst errors that occur during transmission. Frame quality indicator 18 first creates a signal *A* by adding a predetermined number of bits to the end of each frame of input signal *I*. Tail encoder 20 creates a signal *B* by adding a trailing set of 8 bits equal to zero. Convolutional encoder 22 creates a signal *C* with double the bits of signal *B*. An exemplary convolutional encoder is indicated generally at 22a in FIGURE 2. Convolutional encoder 22a includes a linear shift register 34 that receives signal *B* from tail encoder 20. Bit positions 34a, 34b, 34c, 34e, 34g and 34h as well as the current bit of signal *B* are coupled to a modulo-2 adder 36, such as an Exclusive-OR function, to provide a first output of convolutional encoder 22a. Additionally, bit positions 34b, 34c, 34d and 34h as well as the current bit of signal *B* are coupled to a modulo-2 adder 38, such as an Exclusive-OR function, to provide a second output of convolutional encoder 22a. An interleaver 39 interleaves the two outputs of convolutional encoder 22a to provide output signal *C*. Thus, the output bits of convolutional encoder 22a, signal *C*, are a linear combination, e.g. modulo-2 sum, of the bits of signal *B*. Symbol repetition circuit 24 and block interleaver 26 further operate on signal *C* to produce signal *E*. The bits of

signal E are arranged in 16 groups of 24 bits. In the full rate case, the bits of signal E are as shown in TABLE 1 below:

1	9	5	13	3	11	7	15	2	10	6	14	4	12	8	16
65	73	69	77	67	75	71	79	66	74	70	78	68	76	72	80
129	137	133	141	131	139	135	143	130	138	134	142	132	140	136	144
193	201	197	205	195	203	199	207	194	202	198	206	196	204	200	208
257	265	261	269	259	267	263	271	258	266	262	270	260	268	264	272
321	329	325	333	323	331	327	335	322	330	326	334	324	332	328	336
33	41	37	45	35	43	39	47	34	42	38	46	36	44	40	48
97	105	101	109	99	107	103	111	98	106	102	110	100	108	104	112
161	169	165	173	163	171	167	175	162	170	166	174	164	172	168	176
225	233	229	237	227	235	231	239	226	234	230	238	228	236	232	240
289	297	293	301	291	299	295	303	290	298	294	302	292	300	296	304
353	361	357	365	355	363	359	367	354	362	358	366	356	364	360	368
17	25	21	29	19	27	23	31	18	26	22	30	20	28	24	32
81	89	85	93	83	91	87	95	82	90	86	94	84	92	88	96
145	153	149	157	147	155	151	159	146	154	150	158	148	156	152	160
209	217	213	221	211	219	215	223	210	218	214	222	212	220	216	224
273	281	277	285	275	283	279	287	274	282	278	286	276	284	280	288
337	345	341	349	339	347	343	351	338	346	342	350	340	348	344	352
49	57	53	61	51	59	55	63	50	58	54	62	52	60	56	64
113	121	117	125	115	123	119	127	114	122	118	126	116	124	120	128
177	185	181	189	179	187	183	191	178	186	182	190	180	188	184	192
241	249	245	253	243	251	247	255	242	250	246	254	244	252	248	256
305	313	309	317	307	315	311	319	306	314	310	318	308	316	312	320
369	377	373	381	371	379	375	383	370	378	374	382	372	380	376	384

TABLE 1 -- Interleave Pattern of Interleaver 14 for Full Rate Case

It is noted that the numbers in TABLE 1 refer to the bit positions in signal C from convolutional encoder 22. Additionally, each column in TABLE 1 represents one of the 16 groups of 24 bits. The operation of channel coder 12 is public and thus a potential eavesdropper can access the information contained in TABLE 1.

Linear encryptor 16 creates a signal G to be summed (modulo-2) with signal E. Long code generator 26 creates a putatively private long code sequence F from a private long code mask M. An exemplary long code generator indicated generally at 26a is shown in FIGURE 3. Long code generator 26a includes a linear feedback shift register 40 that contains a publicly known quantity having 42 bits. Each bit of the shift register is combined in a corresponding AND-gate 42 with a corresponding bit of the private long code mask M. The output of each AND-gate is coupled to an adder 44. Adder 44 comprises a modulo-2 or Exclusive-OR adder. Adder 44 adds the outputs of and-gates 42

together to produce a bit of the long code sequence F. The relationship between F and M can be expressed as:

$$(1) \qquad F_{f,j} = \sum_i m_i \, x_{i,f,j}$$

where $x_{i,f,j}$ is the content of the i^{th} cell of the linear feedback shift register 40 after having stepped j times during the processing of the f^{th} frame, m_i is the i^{th} bit of the long code mask and $F_{f,j}$ is the j^{th} bit of the long code sequence since the beginning of the f^{th} frame. Decimator 28 outputs 1 in every 64 bits of signal F as signal G which is used to encrypt signal E. Thus, each bit of signal G can also be expressed as:

$$(2) \qquad G_{f,j} = \sum_i m_i \, x_{i,f,(64j)}.$$

Signal E from block interleaver 14 is modulo-2 summed with a signal G of linear encryptor 16 at modulo-2 adder 30. Signal E is added to signal G with modulo-2 arithmetic. For each bit output by modulo-2 adder 30, multiplexer 32 transmits either the output of modulo-2 adder 30 or the PCB signal as the output signal O of forward channel circuit 10. The PCB signal is a power control signal that overwrites a pair of the first 17 bits in each group of 24 bits in signal E. Thus, only the last 7 bits of each group of 24 bits in signal O is free of the effect of the PCB signal.

The long code sequence F used to encrypt the transmission is linearly dependent on the long code mask M (Equation (1)).Further, channel encoder 12 manipulates the bits of input signal I such that the bits of signal D are related to the bits of signal I by known, linear algebraic equations. Thus, if a potential eavesdropper can manipulate the output signal O to remove the effect of the input signal I, the eavesdropper will have data that depends linearly on the unknown bits of the long code mask M. With this data, the eavesdropper can use standard techniques for the solution of linear equations to determine the long code mask M.

The bits of signal E output by channel coder 12 can be combined to create linear equations that depend only on the bits of the long code mask M. To see this relationship, consider the mathematical representation of forward channel circuit 10. First, a bookkeeping detail. Due to the effect of the PCB signal, the only bits that the eavesdropper can rely on are the last 7 bits of each group of 24 bits in output signal O. Thus, in the f^{th} frame, for all bit positions j falling into the last 7 bits of each of the groups of bits, the output of forward channel circuit 10 can be described by the equation:

(3) $E_{f,j} \oplus G_{f,j} = O_{f,j}$.

In each frame, Equation (3) governs the value of 112 bits of signal I input into forward channel circuit 10. Equation (2) above states that G depends on the unknown bits m_i of the long code mask. The vector E is unknown to the eavesdropper. Thus to create an equation that only depends on m_i, the effect of the vector E must be removed. If a vector α can be found such that α_j is zero for all values of j among the first seventeen bits in each group of 24 bits and such that

(4) $<\alpha, E_f> = 0$

then the effect of E on the output vector O can be removed. It is noted that equation (4) refers to the dot product with modulo-2 arithmetic of the vectors α and E. In the vector α, the bits are selected such that the dot product with E creates a sum of bits in E that equal zero. Taking the dot product of each vector in Equation (3) with α produces:

(5) $<\alpha, E_f> \oplus <\alpha, G_f> = <\alpha, O_f>$.

Substituting Equation (4) into equation (5), it is seen that:

(6) $<\alpha, G_f> = <\alpha, O_f>$.

As discussed above in Equation (2), signal G is a decimated version of signal F and each bit is thus linearly dependent on the bits of the long code mask m_i. Equation (6) can thus be expanded as follows:

(7) $$\sum_j \alpha_j G_{f,j} = \sum_j \alpha_j O_{f,j}.$$

Substituting equation (2) into equation (7) reveals that:

(8) $$\sum_j \alpha_j \sum_i m_i x_{i,f,(64\cdot f)} = \sum_j \alpha_j O_{f,j}$$

This is a linear equation wherein the bits m_i of the long code mask are the only unknowns. Thus, the eavesdropper can use known techniques to determine the bits of the long code mask provided enough data is gathered to produce 42 equations. The eavesdropper must

first identify the vectors α that satisfy Equation (3). Channel coder 12 makes this possible.

To find the vectors α that satisfy Equation (3), trace the last 16 bits of data in a signal B through convolutional encoder 22. Assume the last eight bits are 0 as set by tail encoder 20. Further assume that the prior eight bits are a, b, c, d, e, f, g, and h with a being the bit that is followed by the eight zero bits. Then, the last sixteen bits of signal C are:

(9) $c_{369} = a \oplus b \oplus c \oplus e \oplus g \oplus h$;

(10) $c_{370} = b \oplus c \oplus d \oplus h$;

(11) $c_{371} = a \oplus b \oplus d \oplus f \oplus g$;

(12) $c_{372} = a \oplus b \oplus c \oplus g$;

(13) $c_{373} = a \oplus c \oplus e \oplus f$;

(14) $c_{374} = a \oplus b \oplus f$;

(15) $c_{375} = b \oplus d \oplus e$;

(16) $c_{376} = a \oplus e$;

(17) $c_{377} = a \oplus c \oplus d$;

(18) $c_{378} = d$;

(19) $c_{379} = b \oplus c$;

(20) $c_{380} = c$;

(21) $c_{381} = a \oplus b$;

(23) $c_{382} = b$;

(24) $c_{383} = a$; and

(25) $c_{384} = a$.

Combinations of the bits of signal C that yield a modulo-2 sum of zero satisfy Equation (3). For example, the sum of bits c_{383} and c_{384} is zero because the bits are equal. It is noted that after symbol repetition and interleaving bits 383 and 384 of signal C become bits 192 and 384 of signal E, respectively. Thus, a vector α that results in the sum of these two bits will yield a linear equation in the bits m_i of the long code mask M as follows:

(26) $G_{f,192} \oplus G_{f,384} = O_{f,192} \oplus O_{f,384}$.

Equation (26) can be rewritten as:

(27) $$\sum_i m_i (x_{i,f,(64\cdot192)} \oplus x_{i,f,(64\cdot384)}) = O_{f,192} \oplus O_{f,384}$$

In Equation (27), the only unknowns are the bits m_i of the long code mask. Other combinations that result in vectors α are as follows:

(28) $c_{369} \oplus c_{370} \oplus c_{371} \oplus c_{373} \oplus c_{379} \oplus c_{383} = 0$;

(29) $c_{377} \oplus c_{378} \oplus c_{379} \oplus c_{381} = 0$;

(30) $c_{373} \oplus c_{374} \oplus c_{375} \oplus c_{377} \oplus c_{383} = 0$;

(31) $c_{381} \oplus c_{382} \oplus c_{383} = 0$;

(32) $c_{371} \oplus c_{372} \oplus c_{373} \oplus c_{375} \oplus c_{381} = 0$;

(33) $c_{379} \oplus c_{380} \oplus c_{381} \oplus c_{383} = 0$; and

(34) $c_{375} \oplus c_{376} \oplus c_{377} \oplus c_{379} = 0$.

Thus, in the full rate case, the eavesdropper can create at least eight combinations of bits from one frame of data that cancel the effect of the input signal I on the output signal O. With just six frames of data the eavesdropper can create more than the 42 equations necessary to determine the value of the 42 bits of the long code mask M. This data can be gathered in less than one second. In the lower rate cases, the task of the eavesdropper is somewhat simplified. TABLE 2 below shows the bits of signal E with the number of the bit position for each bit as in signal C output by the convolutional encoder.

1	2	1	2	1	2	1	2	1	2	1	2	1	2	1	2
9	10	9	10	9	10	9	10	9	10	9	10	9	10	9	10
17	18	17	18	17	18	17	18	17	18	17	18	17	18	17	18
25	26	25	26	25	26	25	26	25	26	25	26	25	26	25	26
33	34	33	34	33	34	33	34	33	34	33	34	33	34	33	34
41	42	41	42	41	42	41	42	41	42	41	42	41	42	41	42
5	6	5	6	5	6	5	6	5	6	5	6	5	6	5	6
13	14	13	14	13	14	13	14	13	14	13	14	13	14	13	14
21	22	21	22	21	22	21	22	21	22	21	22	21	22	21	22
29	30	29	30	29	30	29	30	29	30	29	30	29	30	29	30
37	38	37	38	37	38	37	38	37	38	37	38	37	38	37	38
45	46	45	46	45	46	45	46	45	46	45	46	45	46	45	46
3	4	3	4	3	4	3	4	3	4	3	4	3	4	3	4
11	12	11	12	11	12	11	12	11	12	11	12	11	12	11	12
19	20	19	20	19	20	19	20	19	20	19	20	19	20	19	20
27	28	27	28	27	28	27	28	27	28	27	28	27	28	27	28
35	36	35	36	35	36	35	36	35	36	35	36	35	36	35	36
43	44	43	44	43	44	43	44	43	44	43	44	43	44	43	44
7	8	7	8	7	8	7	8	7	8	7	8	7	8	7	8
15	16	15	16	15	16	15	16	15	16	15	16	15	16	15	16
23	24	23	24	23	24	23	24	23	24	23	24	23	24	23	24
31	32	31	32	31	32	31	32	31	32	31	32	31	32	31	32
39	40	39	40	39	40	39	40	39	40	39	40	39	40	39	40
47	48	47	48	47	48	47	48	47	48	47	48	47	48	47	48

TABLE 2 – Interleave Pattern of Interleaver 14 for Low Rate Case

It is noted that each bit is repeated eight times. Thus, in the low rate case, the eavesdropper can determine the bits of the long code mask M with a single frame of data. Thus, it is easier in the low rate case to create equations to determine the bits of the long code mask M.

FIGURE 4 is a block diagram of a wireless system indicated generally at 110 that implements a spread spectrum technology and is constructed according to the teachings of the present invention. Wireless system 110 includes a plurality of base stations 112 that are coupled to and in communication with a Mobile Switching Center (MSC) 114. MSC 114 is coupled to and in communication with the public switched telephone network (PSTN) 116, including one or more local offices 118 and one or more toll offices 120. PSTN 116 further includes fixed terminals 122 coupled to and in communication with local offices 118 and toll offices 120. Fixed terminals may be

coupled to PSTN by any appropriate telecommunications cable including, for example, copper wires, fiber optic cables and the like. Wireless system 110 also includes one or more wireless terminals 124. The forward channel of each wireless terminal 124 and each base station 112 includes an encryptor as described below for providing increased transmission privacy when compared to prior systems and methods.

In operation, wireless system 110 transmits an encrypted signal between a base station 112 and a wireless terminal 124. For example, a communication to a wireless terminal 124 may be initiated at a fixed terminal 122. Local office 118 and MSC 114 connect fixed terminal 122 to an appropriate base station 112. Base station 112 encrypts a signal from fixed terminal 122 and transmits the encrypted signal. The appropriate wireless terminal 124 receives the encrypted signal. Wireless terminal 124 decrypts the signal to complete the communication.

FIGURE 5 is a block diagram of one embodiment of a base station indicated generally at 112 and constructed according to the teachings of the present invention. Base station 112 includes a forward channel 126 for transmitting signals to a wireless terminal 124. Base station 112 also includes a reverse channel 128 for receiving signals from a wireless terminal 124. Forward channel 126 includes an encryptor 130 that createsa key signal that is a nonlinear function of a private long code mask. Thus, forward channel 126 provides increased transmission privacy.

Forward channel 126 includes a channel coder 132 that is coupled to MSC 114. Forward channel 126 further includes the series combination of bit interleaver 134, encryptor 130, Walsh function modulator 136, quadrature spreader 138, quadrature carrier modulator 140, and RF transmitter 142. RF transmitter 142 is coupled to antenna 144. Reverse channel 128 includes the series combination of RF receiver 146, quadrature carrier demodulator 148, quadrature despreader 150, despreader 152, Walsh symbol demodulator 154, bit deinterleaver 156, and channel decoder 158.

In operation, forward channel 126 processes and encrypts a signal from MSC 114 for transmission on antenna 144. MSC 114 provides a digital signal to channel coder 132. Channel coder 132 codes the signal for error correction after transmission. Bit interleaver 134 rearranges the order of the bits in the signal so as to minimize the impact of error bursts. Encryptor 130 uses a nonlinear encryption signal to encrypt the signal from bit interleaver 134. Walsh function modulator 136 modulates the signal by multiplying the signal with a selected Walsh function. Quadrature spreader 138 spreads the signal with a selected pseudo-noise (PN) code that is unique to the transmission between fixed terminal 122 and wireless terminal 124. Quadrature carrier modulator 140 modulates the signal for transmission by RF transmitter 142 on antenna 144.

Reverse channel 128 receives a signal from a wireless terminal 124 at antenna 144 and receiver 146. Quadrature carrier demodulator 148 demodulates the signal from the carrier signal for processing. Quadrature despreader 150 uses the appropriate PN signal to despread the signal from wireless terminal 124. Despreader 152 uses a private key signal to further despread the signal from wireless terminal 124. Walsh symbol demodulator 154 demodulates the signal with an appropriate Walsh function. Bit deinterleaver 156 rearranges the bits in the signal to undo an interleaving operation performed by wireless terminal 124. Channel decoder 158 uses error correction techniques to correct errors in the signal from wireless terminal 124.

FIGURE 6 is a block diagram of a wireless terminal indicated generally at 124 and constructed according to the teachings of the present invention. Wireless terminal 124 includes a reverse channel 160 for transmitting signals to a base station 112. Wireless terminal 124 also includes a forward channel 162 for receiving signals from a base station 112. Forward channel 162 includes a decryptor 164 that creates a key signal that is a nonlinear function of a private long code mask. Thus, forward channel 162 provides increased transmission privacy.

Wireless terminal 168 includes an input/output (I/O) device 166. I/O device 166 may comprise a speaker and a microphone. Alternatively, I/O device 166 may comprise an appropriate data port. Reverse channel 160 includes a voice coder 168 coupled to I/O device 166. Voice coder 168 is coupled to the series combination of channel coder 170, bit interleaver 172, Walsh function modulator 174, spreader 176, quadrature spreader 178, quadrature carrier modulator 180, and RF transmitter 182. RF transmitter 182 is coupled to antenna 184. Reverse channel 162 includes the series combination of RF receiver 186, quadrature carrier demodulator 188, quadrature despreader 190, Walsh function demodulator 192, decryptor 164, bit deinterleaver 194, channel decoder 196 and voice decoder 198. Voice decoder 198 is coupled to I/O device 166.

In operation, reverse channel 160 processes a signal from a user for transmission on antenna 184. Voice coder 168 codes a digital signal from I/O device 166. Channel coder 170 codes the signal for error correction after transmission. Bit interleaver 172 rearranges the order of the bits in the signal so as to minimize the impact of error bursts. Walsh function modulator 174 modulates the signal by multiplying the signal with a selected Walsh function. Spreader 176 usesa key signal to spread the signal from Walsh function modulator 174. Quadrature spreader 178 spreads the signal with a selected pseudo-noise (PN) code that is unique to the transmission between fixed terminal 122 and

wireless terminal 124. Quadrature carrier modulator 180 modulates the signal for transmission by RF transmitter 182 on antenna 184.

Forward channel 162 receives a signal from base station 112 at antenna 184 and receiver 186. Quadrature carrier demodulator 188 demodulates the signal from the carrier signal for processing. Quadrature despreader 190 uses the appropriate PN signal to despread the signal from base station 112. Walsh function demodulator 192 demodulates the signal with an appropriate Walsh function. Decryptor 164 uses a private key signal to descramble the signal from base station 112. Bit deinterleaver 194 rearranges the bits in the signal to undo an interleaving operation performed by base station 112. Channel decoder 196 uses error correction techniques to correct errors in the signal from base station 112. Voice decoder 198 decodes the signal for I/O device 166 to complete the transmission.

FIGURE 7 is an embodiment of an encryptor indicated generally at 130 for use in forward channel 126 of FIGURE 5. Encryptor 130 generates a key signal with the series combination of a long code generator 200, a nonlinear scrambler 202 and a decimator 204. The output of decimator 204 is coupled to a first input of a modulo-2 adder 206. The second input of adder 206 is coupled to bit interleaver 134.

In operation, long code generator 200 generates a sequence of bits from a private long code mask. Long code generator 200 may comprise the long code generator 22a of FIGURE 3 such that the bits of the long code sequence depend linearly on the bits of the long code mask. Nonlinear scrambler 202 scrambles the bits of the long code sequence such that the output bits of nonlinear scrambler 202 have a nonlinear dependence on the bits of the long code mask. Exemplary embodiments of nonlinear scrambler 202 are described below with respect to FIGUREs 9 through 15. The nonlinearity created by nonlinear scrambler 202 may vary in complexity. For example, nonlinear scrambler 202 may include a feedback loop. Alternatively, nonlinear scrambler 202 may comprise a simple combinational logic circuit that introduces a nonlinearity into the long code sequence. Thus, a system constructed according to the teachings of the present invention will increase the difficulty for an eavesdropper to successfully obtain the bits of the long code mask M. Decimator 204 selects bits output from nonlinear scrambler 202 with a known frequency. For example, decimator 204 may output 1 in 64 of the bits output by nonlinear scrambler 202. Adder 206 adds (modulo-2) the signal from bit interleaver 134 with the signal from decimator 204.

FIGURE 8 is an embodiment of a decryptor indicated generally at 164 for use in forward channel 162 of FIGURE 6. Decryptor 164 generates a key signal with the series combination of a long code generator 208, a nonlinear scrambler 210 and a

decimator 212. The output of decimator 212 is coupled to a first input of a modulo-2 adder 214. The second input of adder 214 is coupled to Walsh function demodulator 192.

In operation, decryptor 164 creates a key signal to decrypt a signal received from a base station 112. As such, decryptor 164 independently creates a key signal that is identical to the key signal created in encryptor 130. Thus, long code generator 208 generates a sequence of bits from a private long code mask. Long code generator 208 may comprise the long code generator 22a of FIGURE 3 such that the bits of the long code sequence depend linearly on the bits of the long code mask. Nonlinear scrambler 210 scrambles the bits of the long code sequence such that the output bits of nonlinear scrambler 210 have a nonlinear dependence on the bits of the long code mask. Exemplary embodiments of nonlinear scrambler 210 are described below with respect to FIGUREs 9 through 15. The nonlinearity created by nonlinear scrambler 210 may vary in complexity. For example, nonlinear scrambler 210 may include a feedback loop. Alternatively, nonlinear scrambler 210 may comprise a simple combinational logic circuit that introduces a nonlinearity into the long code sequence. Thus, a system constructed according to the teachings of the present invention will increase the difficulty for an eavesdropper to successfully obtain the bits of the long code mask M. Decimator 212 selects bits output from nonlinear scrambler 210 with a known frequency. For example, decimator 212 may output 1 in 64 of the bits output by nonlinear scrambler 210. Adder 214 adds the signal from Walsh function demodulator 192 with the signal from decimator 212.

FIGURE 9 is one embodiment of a nonlinear scrambler indicated generally at 202a and constructed according to the teachings of the present invention. It is noted that each circuit shown in FIGUREs 9 through 15 can be used either in encryptor 130 or decryptor 164. For simplicity, FIGUREs 9 through 15 are described only with respect to encryptor 130. Scrambler 202a comprises an Exclusive-OR gate 216, a shift register 218, a logic circuit 220 and a switch 222. The output of long code generator 200 and the output of logic circuit 220 are coupled to the inputs of Exclusive-OR gate 216. Exclusive-OR gate 216 provides an output to shift register 218 and to switch 222. Logic circuit 220 taps two or more cells of shift register 218. Finally, the output of long code generator 200 is also coupled to switch 222.

In operation, scrambler 202a outputs a sequence of bits that are a nonlinear combination of the bits of the long code sequence by use of a feedback loop. Exclusive-OR gate 216 outputs bits to shift register 218. The bits shift through shift register 218 and are selectively combined in logic circuit 220. Logic circuit 220 may comprise a simple AND-gate. Alternatively, logic circuit 220 may comprise a more complicated

combinational logic circuit. Logic circuit 220 provides a second input to Exclusive-OR gate 216 such that the bits entering shift register 218 ultimately depend on the current bit of the long code sequence and a logical combination of prior bits output by Exclusive-OR gate 216. Switch 222 may by-pass the effect of scrambler 202a by coupling long code generator 200 directly to decimator 204. A reset signal is also provided to clear shift register 218.

FIGURE 10 illustrates another embodiment of a nonlinear scrambler indicated generally at 202b constructed according to the teachings of the present invention. Scrambler 202b comprises a shift register 224 having 64 cells. Each cell of shift register 224 is coupled to an input of a multiplexer 226. Additionally, the cells labeled 0 through 5 of shift register 224 are coupled to selector inputs of multiplexer 226. It is noted that any six of the cells of shift register 224 could be used as the selector inputs for multiplexer 226.

In operation, the bits of the long code sequence shift through shift register 224. The values in cells 0 through 5 of shift register 224 select one of the cells from shift register 224 to be passed as an output bit by multiplexer 226 to decimator 204.

FIGURE 11 illustrates another embodiment of a nonlinear scrambler indicated generally at 202c and constructed according to the teachings of the present invention. Scrambler 202c comprises a shift register 228 having 64 cells. N selected cells of shift register 228 are coupled to selector inputs of multiplexer 230. Additionally, 2^N selected cells of shift register 228 are also coupled as inputs of multiplexer 230.

In operation, the bits of the long code sequence shift through shift register 228. Multiplexer 230 selects a cell of shift register 228 based on the selector inputs from shift register 228. The value of the selected cell is passed as the output of scrambler 202c to decimator 204.

FIGURE 12 illustrates another embodiment of a nonlinear scrambler indicated generally at 202d constructed according to the teachings of the present invention. Scrambler 202d comprises a shift register 232 having 64 cells. Each cell of shift register 232 is coupled to an input of data encryption standard (DES) circuit 234. DES circuit 234 encrypts data according to Federal Information Processing Standards Publication 46 dated January 15, 1977. A private key signal is provided to DES circuit 234. DES circuit 234 comprises 64 outputs that are coupled to a register 236. A selected cell of register 236 is provided as an output for scrambling circuit 202d.

In operation, the bits of the long code sequence shift through shift register 232. DES circuit 234 encrypts the data in shift register 232 using the key signal and conventional DES techniques. DES circuit 234 provides an encrypted version of the data

in shift register 232 to register 236. Scrambler 202d provides an output signal from register 236 to decimator 204.

FIGURE 13 illustrates another embodiment of a nonlinear scrambler indicated generally at 202e and constructed according to the teachings of the present invention. Scrambler 202e comprises a shift register 240 having 64 cells. N selected cells of shift register 240 are coupled to inputs of a nonlinear function 242. For example, nonlinear function 242 may comprise a two input AND-gate or other appropriate function for creating a nonlinear output.

In operation, the bits of the long code sequence shift through shift register 240. Nonlinear function 242 generates an output signal based on the values of the N input cells of shift register 240.

FIGURE 14 is another embodiment of a nonlinear scrambler indicated generally at 202f and constructed according to the teachings of the present invention. Scrambler 202f comprises an Exclusive-OR gate 244, a shift register 246, a first logic circuit 248 and a second logic circuit 250. The output of long code generator 200 and the output of first logic circuit 248 are coupled to the inputs of Exclusive-OR gate 244. Exclusive-OR gate 244 is coupled to shift register 246. First logic circuit 248 taps two or more cells of shift register 246. Finally, second logic circuit 250 taps a second selected set of cells of shift register 246. Second logic circuit 250 comprises the output of scrambler 202f. A reset signal is also provided to clear shift registers 248 and 250.

In operation, scrambler 202f outputs a sequence of bits that are a nonlinear combination of the bits of the long code sequence by use of a feedback loop. Exclusive-OR gate 244 outputs bits to shift register 246. The bits shift through shift register 246 and are selectively combined in first logic circuit 248. First logic circuit 248 may comprise a simple AND-gate. Alternatively, first logic circuit 248 may comprise a more complicated combinational logic circuit. First logic circuit 248 provides a second input to Exclusive-OR gate 244 such that the bits entering shift register 246 ultimately depend on the current bit of the long code sequence and a logical combination of prior bits output by Exclusive-OR gate 244. Second logic circuit 250 combines bits from selected cells of register 246 as output for scrambler 202f.

FIGURE 15 is another embodiment of a nonlinear scrambler indicated generally at 202g and constructed according to the teachings of the present invention. Scrambler 202g comprises an Exclusive-OR gate 252, a shift register 254, a first logic circuit 256 and a second logic circuit 258. The output of long code generator 200 and the output of first logic circuit 256 are coupled to the inputs of Exclusive-OR gate 252. Exclusive-OR gate 252 is coupled to shift register 254. First logic circuit 256 taps one or

more cells of shift register 256. Additionally, a private key signal K_1 may be provided to first logic circuit 256 for use in creating the encryption signal. Second logic circuit 258 taps a second selected set of cells of shift register 254. A second private key K_2 may be provided to second logic circuit 258 for use in creating the encryption signal. Second logic circuit 258 comprises the output of scrambler 202g. A reset signal is also provided to clear shift registers 256 and 258.

In operation, scrambler 202g outputs a sequence of bits that have a nonlinear dependence on a private sequence of bits. The private sequence of bits can be the long code mask as processed by long code generator 202, signal K_1 or K_2, or any appropriate combination thereof. Exclusive-OR gate 252 outputs bits to shift register 254. The bits shift through shift register 254 and are selectively combined with bits of signal K_1 in first logic circuit 256. First logic circuit 248 may comprise a simple and-gate. Alternatively, first logic circuit 256 may comprise a more complicated combinational logic circuit. First logic circuit 256 provides a second input to Exclusive-OR gate 252 such that the bits entering shift register 254 ultimately depend on the current bit of the long code sequence and a logical combination of prior bits output by Exclusive-OR gate 252 and the signal K_1. Second logic circuit 258 combines bits from selected cells of register 254 with bits of signal K_2 as output for scrambler 202f.

It is noted that nonlinear scrambler 202g can achieve increased privacy over conventional systems without use of long code generator 200. If long code generator 200 is omitted from encryptor 130, either K_1, K_2 or both must be private to increase privacy. Additionally, if either K_1, K_2 or both are private, long code generator 200 could create a long code sequence from a public long code mask M. It is also noted that either K_1 or K_2 may be omitted without departing from the teachings of the present invention.

FIGURE 16 is another embodiment of an encryptor indicated generally at 130a for use in the base station 112 of FIGURE 5. Encryptor 130a generates a key signal with the series combination of a shift register 260 and, a nonlinear combiner 262 and a decimator 264. The output of decimator 264 is coupled to a first input of a modulo-2 adder 266. The second input of adder 266 is coupled to bit interleaver 134. A private long code mask, *M*, is provided to nonlinear combiner 262.

In operation, ecryptor 130a generates a key signal with bits that are a nonlinear combination of the bits of the long code mask. Shift register 260 generates a sequence of bits from a publicly known quantity. Nonlinear combiner 262 combines the long code mask *M* with the output of shift register 260. Decimator 264 selects bits output from nonlinear combiner 262 with a known frequency. For example, decimator 264 may

output 1 in 64 of the bits output by nonlinear combiner 262. Adder 266 adds (modulo-2) the signal from bit interleaver 134 with the signal from decimator 264.

FIGURE 17 is another embodiment of a decryptor indicated generally at 164a for use in the wireless terminal 124 of FIGURE 6. Decryptor 164a generates a key signal with the series combination of a shift register 268, a nonlinear combiner 270 and a decimator 272. The output of decimator 272 is coupled to a first input of a modulo-2 adder 274. The second input of adder 274 is coupled to Walsh symbol demodulator 154. A private long code mask, M, is provided to nonlinear combiner 270.

In operation, decryptor 164a generates a key signal with bits that are a nonlinear combination of the bits of the long code mask. Shift register 268 generates a sequence of bits from a publicly known quantity. Nonlinear combiner 270 combines the long code mask M with the output of shift register 268. Decimator 272 selects bits output from nonlinear combiner 270 with a known frequency. For example, decimator 272 may output 1 in 64 of the bits output by nonlinear combiner 270. Adder 274 adds (modulo-2) the signal from Walsh symbol modulator 154 with the signal from decimator 272.

Although the present invention has been described in detail, it should be understood that various alterations, substitutions and changes can be made hereto without departing from the spirit and scope of the invention as defined by the appended claims. For example, the shift registers shown in FIGUREs 9 through 15 are not limited to 64 cells. The number of cells may be varied without departing from the teachings of the present invention. The 64 cell registers are simply shown by way of example and not by way of limitation. Furthermore, the encryptors and decryptors described herein can be used without decimators. Alternatively, the function of decimator can be partially or fully incorporated into other circuitry.

Scramblers 202a through 202g each includes one or more shift registers. It is emphasized that these shift registers are shown by way of example and not by way of limitation. The shift registers store input bits provided to the scrambler for use in creating subsequent output bits. To this end, the shift registers in FIGUREs 9 through 15 can be replaced with any appropriate circuit for performing this same function.

To ensure that the nonlinear scramblers constructed according to the teachings of the present invention in the base station and in the wireless terminal produce identical outputs when fed with identical long code sequence inputs during a transmission, the scramblers should start with the same internal state. Thus, any shift registers in the scramblers must start with identical contents. One means for accomplishing this is to reset any such shift registers with fixed initial values in response to a reset signal during the time of hand-off. The reset signals shown in FIGUREs 9, 14 and 15 can be used to implement

this feature. The registers may also be reset, for example, such as at the beginning of each new frame.

It is noted that the Exclusive-OR gates specified in FIGUREs 9, 14 and 15 can be implemented with any appropriate function that performs modulo-2 addition.

It is also noted that the number of bits in the long code mask may be varied from 42 without departing from the spirit and scope of the teachings of the present invention.

4. Brief Description of Drawings

FIGURE 1 is a block diagram of a forward channel circuit of a spread spectrum wireless system according to a draft standard published in December 1994 as PN-3421 by the Telecommunications Industry Association;

FIGURE 2 is a block diagram of a convolution encoder for use in the forward channel circuit of FIGURE 1;

FIGURE 3 is a block diagram of an embodiment of a long code generator for use in the forward channel circuit of FIGURE 1;

FIGURE 4 is a block diagram of a spread spectrum wireless infrastructure incorporating a nonlinear scrambler constructed according to the teachings of the present invention;

FIGURE 5 is a block diagram of a base station in the spread spectrum wireless system of FIGURE 4;

FIGURE 6 is a block diagram of a wireless terminal in the spread spectrum wireless system of FIGURE 4;

FIGURE 7 is an embodiment of an encryptor for use in the base station of FIGURE 5;

FIGURE 8 is an embodiment of a decryptor for use in the wireless terminal of FIGURE 6;

FIGURE 9 is an embodiment of a nonlinear scrambler for use in the encryptor of FIGURE 7 and the decryptor of FIGURE 8;

FIGURE 10 is another embodiment of a nonlinear scrambler for use in the encryptor of FIGURE 7 and the decryptor of FIGURE 8;

FIGURE 11 is another embodiment of a nonlinear scrambler for use in the encryptor of FIGURE 7 and the decryptor of FIGURE 8;

FIGURE 12 is another embodiment of a nonlinear scrambler for use in the encryptor of FIGURE 7 and the decryptor of FIGURE 8;

FIGURE 13 is another embodiment of a nonlinear scrambler for use in the encryptor of FIGURE 7 and the decryptor of FIGURE 8;

FIGURE 14 is another embodiment of a nonlinear scrambler for use in the encryptor of FIGURE 7 and the decryptor of FIGURE 8;

FIGURE 15 is another embodiment of a nonlinear scrambler for use in the encryptor of FIGURE 7 and the decryptor of FIGURE 8;

FIGURE 16 is another embodiment of an encryptor for use in the base station of FIGURE 5; and

FIGURE 17 is another embodiment of a decryptor for use in the wireless terminal of FIGURE 6.

FIG. 1

(prior art)

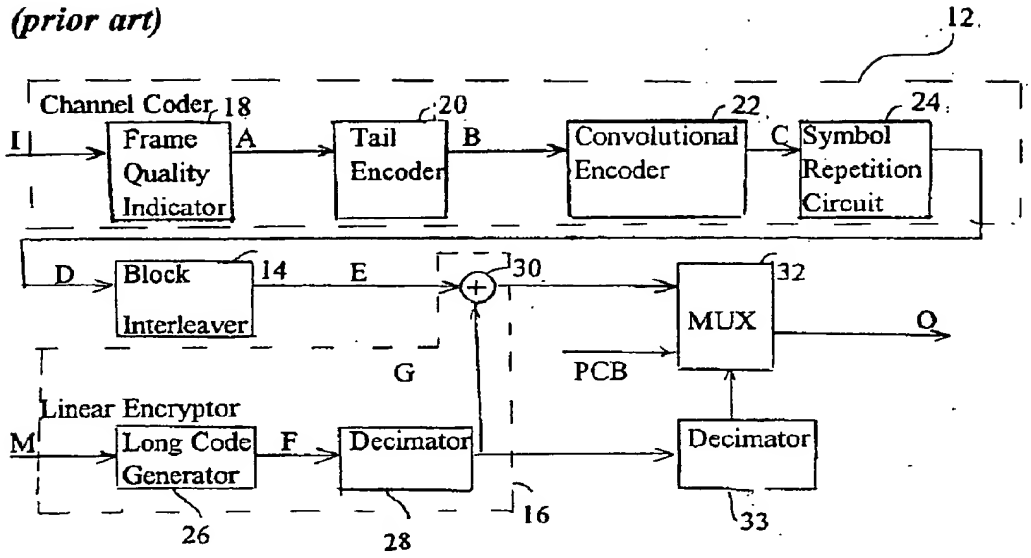


FIG. 2

(prior art)

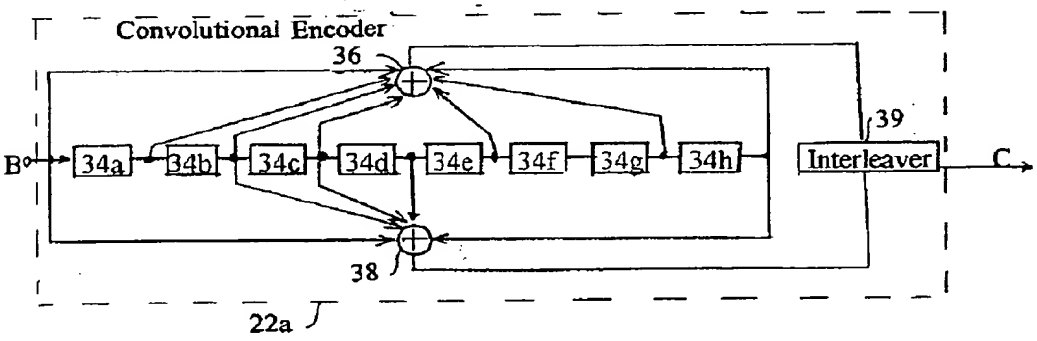


FIG. 3

(prior art)

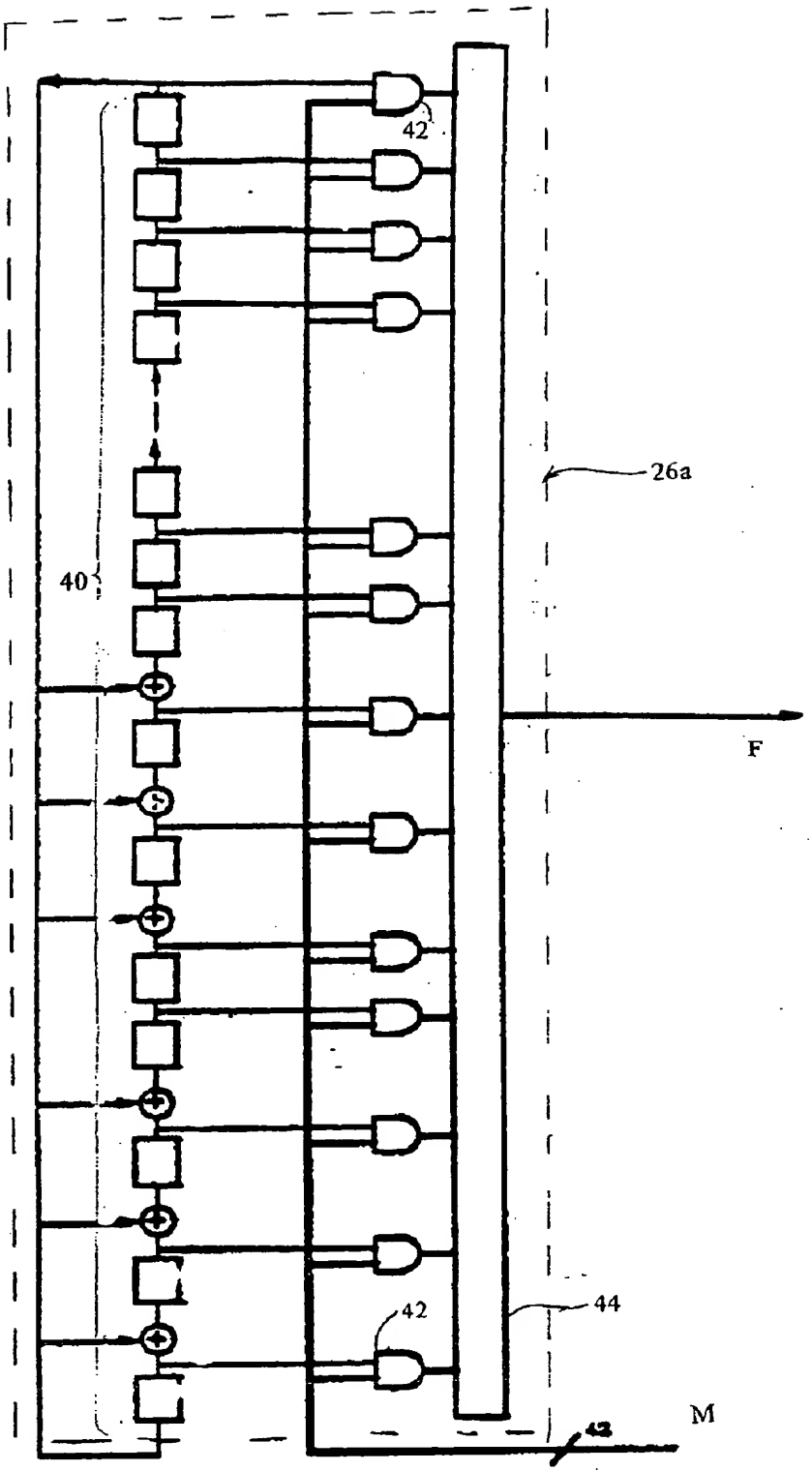


FIG. 4

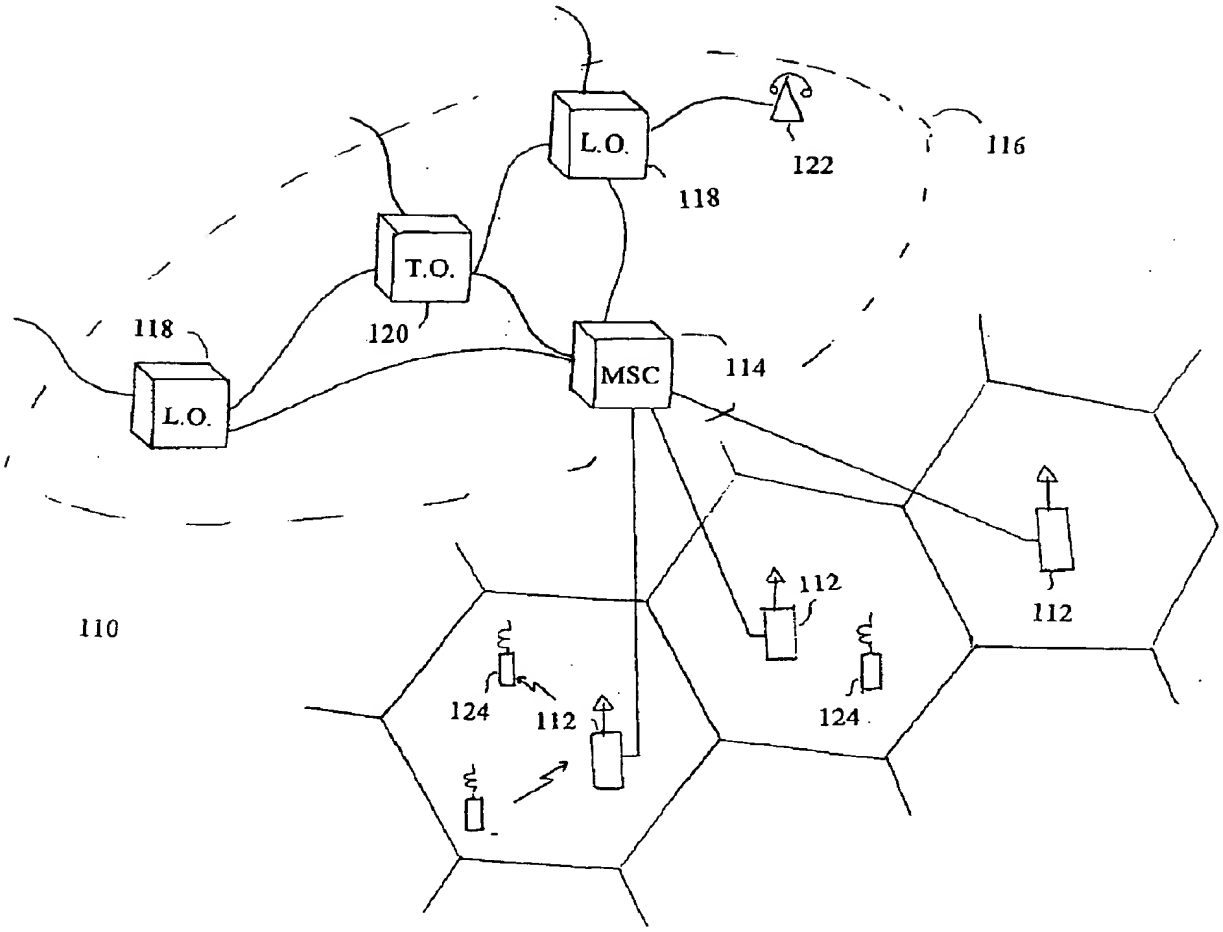


FIG. 5

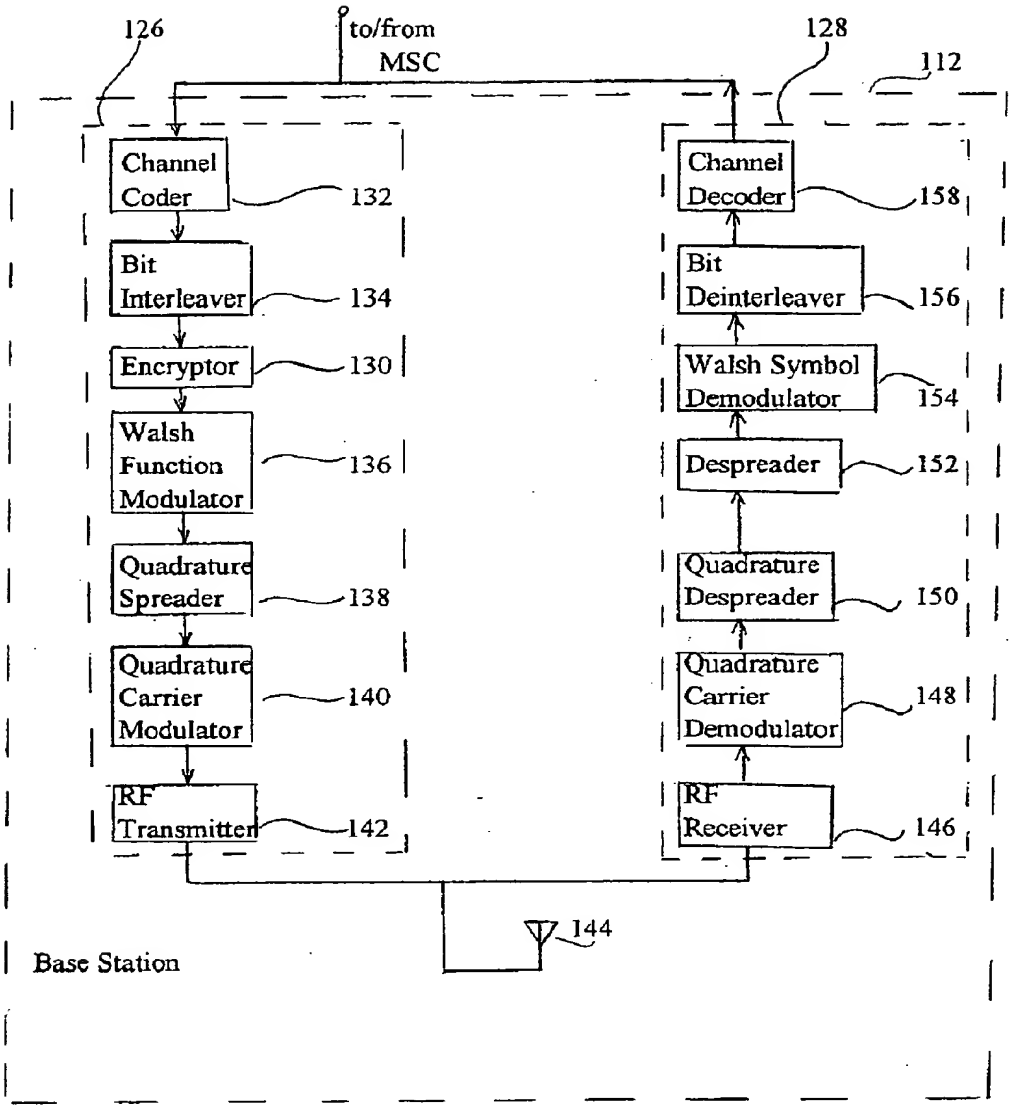

126
to/from MSC
128
112
Channel Coder
132
Bit Interleaver
134
Encryptor
130
Walsh Function Modulator
136
Quadrature Spreader
138
Quadrature Carrier Modulator
140
RF Transmitter
142
Channel Decoder
158
Bit Deinterleaver
156
Walsh Symbol Demodulator
154
Despreader
152
Quadrature Despreader
150
Quadrature Carrier Demodulator
148
RF Receiver
146
144
Base Station

FIG. 6

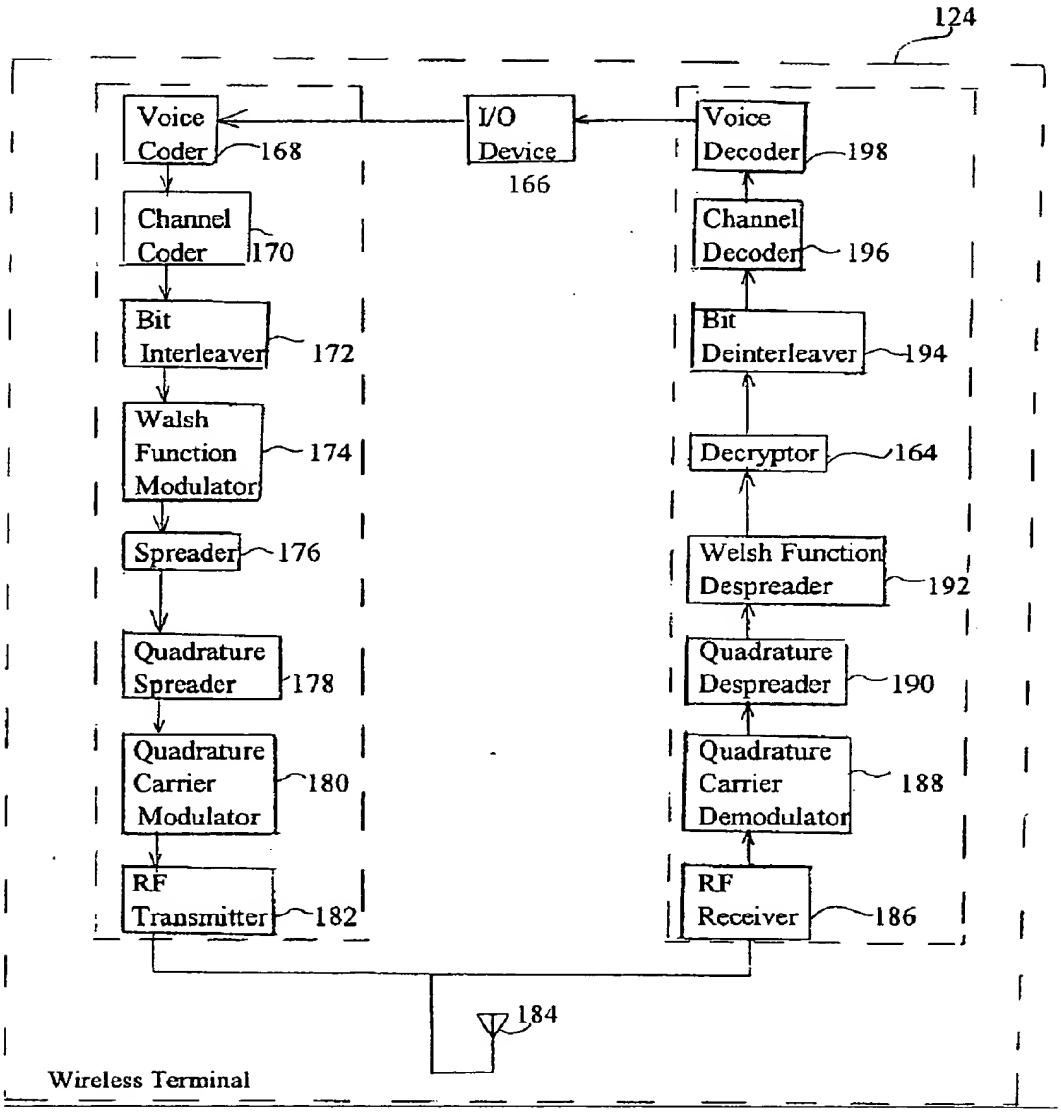

124
Voice Coder
168
I/O Device
166
Voice Decoder
198
Channel Coder
170
Channel Decoder
196
Bit Interleaver
172
Bit Deinterleaver
194
Walsh Function Modulator
174
Decryptor
164
Spreader
176
Welsh Function Despreader
192
Quadrature Spreader
178
Quadrature Despreader
190
Quadrature Carrier Modulator
180
Quadrature Carrier Demodulator
188
RF Transmitter
182
RF Receiver
186
184
Wireless Terminal

FIG. 7

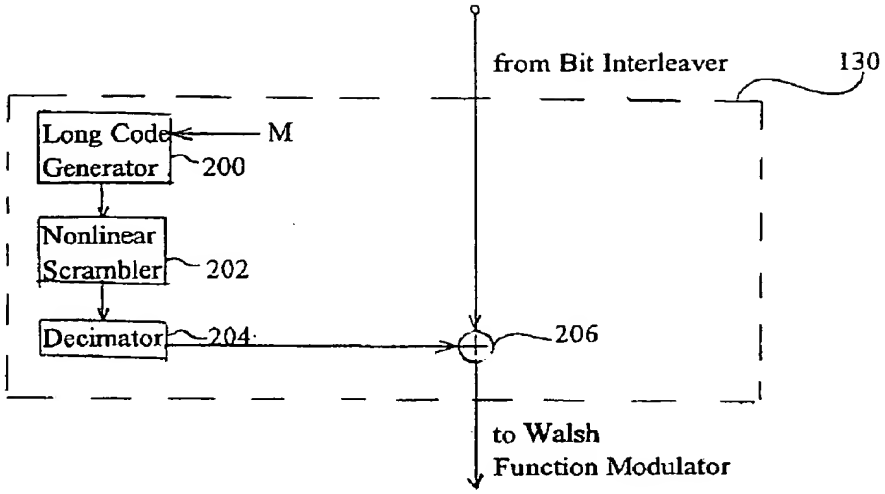

from Bit Interleaver
130
Long Code Generator
M
200
Nonlinear Scrambler
202
Decimator
204
206
to Walsh Function Modulator

FIG. 8

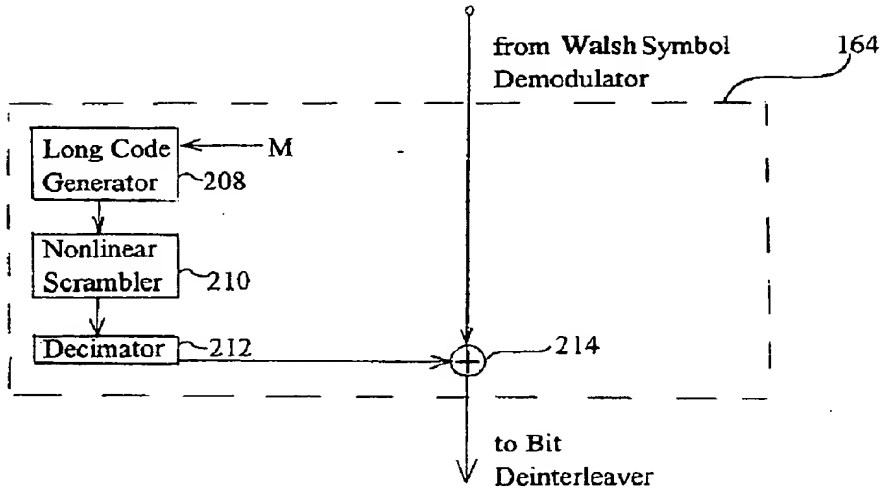

from Walsh Symbol Demodulator
164
Long Code Generator
M
208
Nonlinear Scrambler
210
Decimator
212
214
to Bit Deinterleaver

FIG. 9

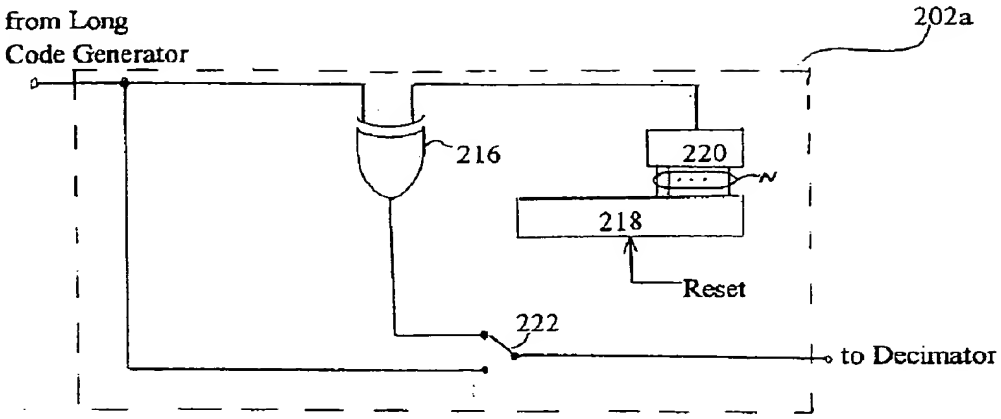

from Long
Code Generator
202a
216
220
218
Reset
222
to Decimator

FIG. 10

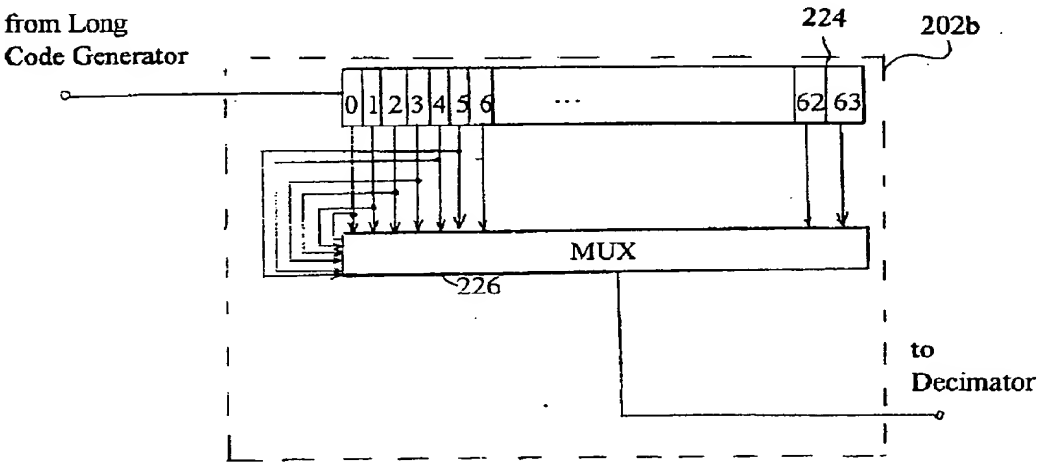

from Long
Code Generator
224
202b
0 1 2 3 4 5 6 ... 62 63
MUX
226
to
Decimator

FIG. 11

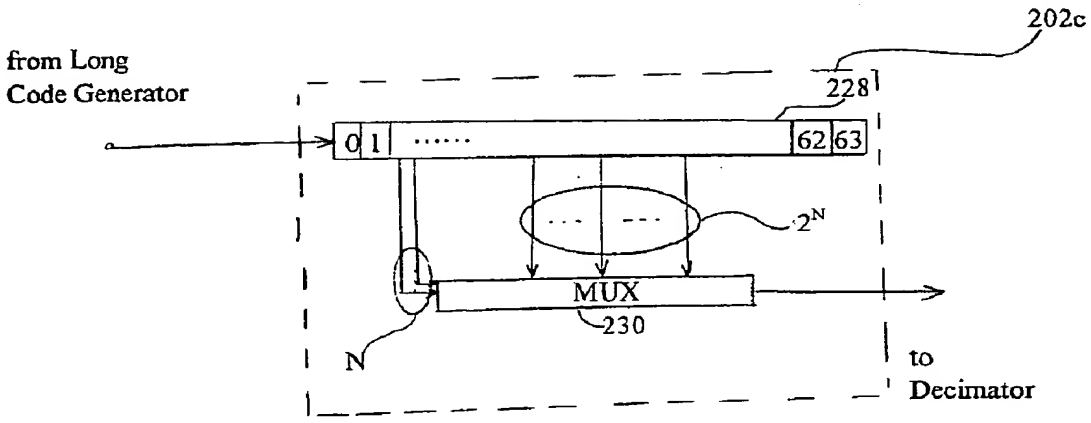

202c
from Long
Code Generator
228
0
1
62
63
2^N
MUX
230
N
to
Decimator

FIG. 12

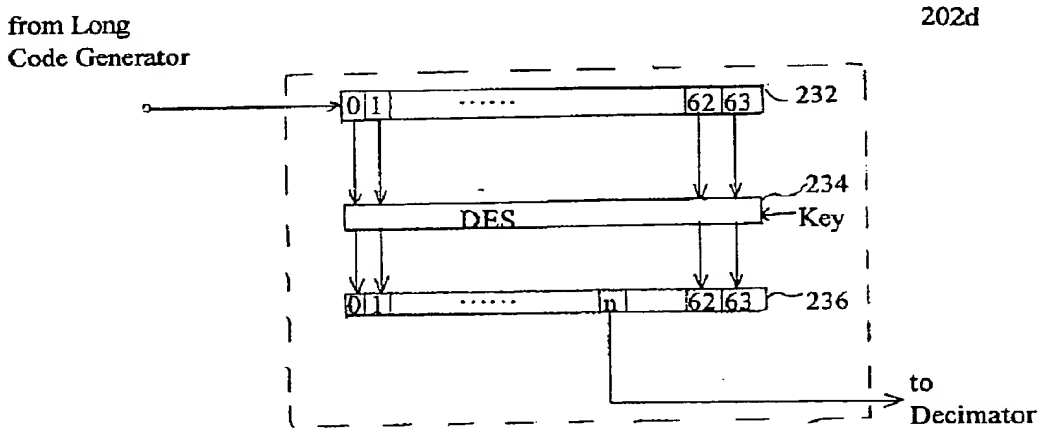

202d
from Long
Code Generator
0
1
62
63
232
234
DES
Key
n
236
to
Decimator

FIG. 13

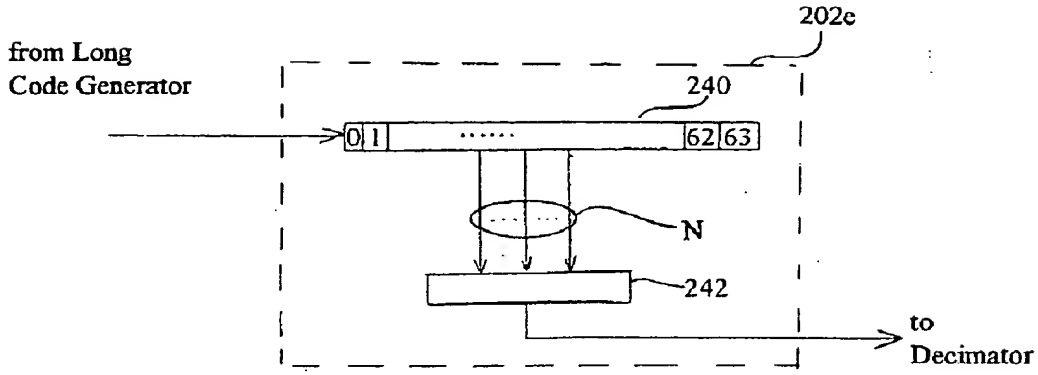

202e
from Long
Code Generator
240
0
1
62
63
N
242
to
Decimator

FIG. 14

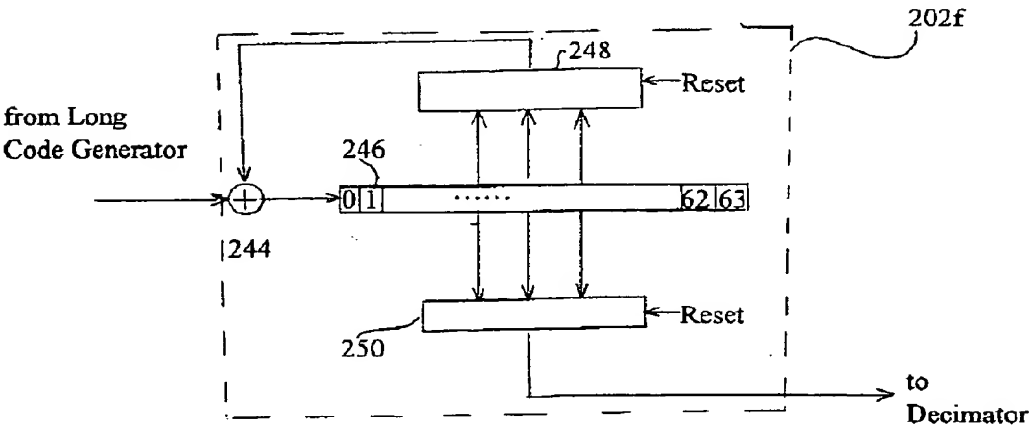

202f
248
Reset
from Long
Code Generator
246
0
1
62
63
244
Reset
250
to
Decimator

FIG. 15

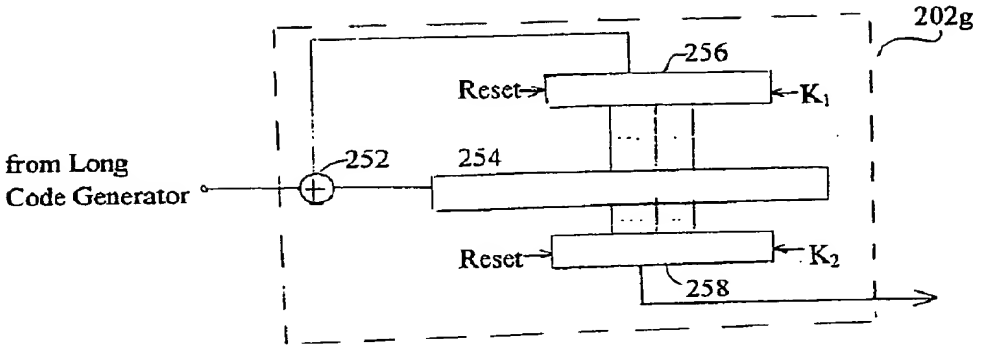


FIG. 16

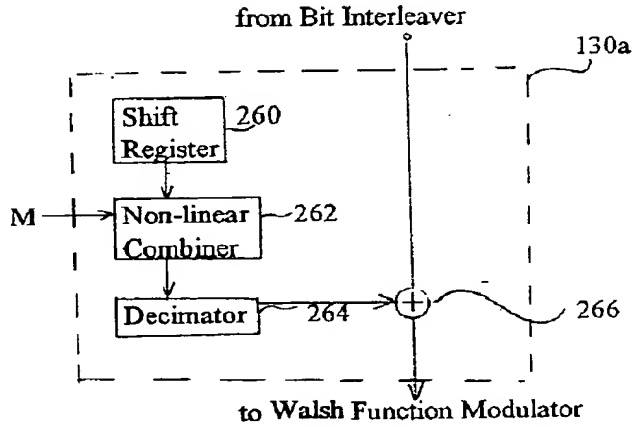
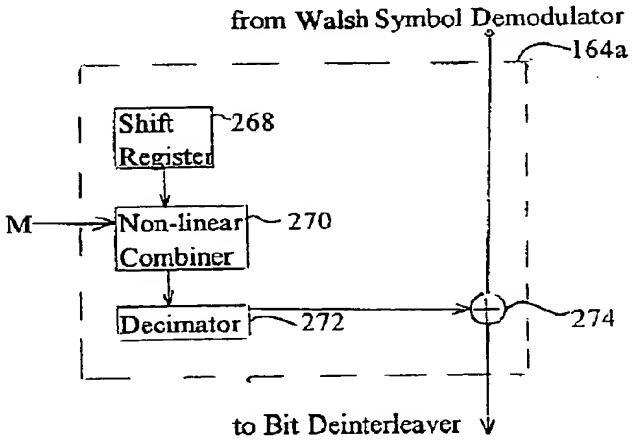


FIG. 17



1. Abstract

A wireless communication system (110) with increased privacy. The system (110) transmits an encrypted signal between a base station (112) and a wireless terminal (122). In the forward channel, the base station (112) includes an encryptor (130) with a nonlinear scrambler (202) that creates an key signal that has a nonlinear dependence on a long code mask M. The wireless terminal (122) similarly includes a decryptor (164) with a nonlinear scrambler (210) that creates a key signal that has a nonlinear dependence on the long code mask M.

2. Representative Drawing

Figure 4.